

AN ARITHMETIC INTERSECTION FORMULA ON HILBERT MODULAR SURFACES

TONGHAI YANG

ABSTRACT. In this paper, we obtain an explicit arithmetic intersection formula on a Hilbert modular surface between the diagonal embedding of the modular curve and a CM cycle associated to a non-biquadratic CM quartic field. This confirms a special case of the author's conjecture with J. Bruinier in [BY], and is a generalization of the beautiful factorization formula of Gross and Zagier on singular moduli. As an application, we proved the first non-trivial non-abelian Chowla-Selberg formula, a special case of Colmez conjecture.

1. INTRODUCTION

Intersection theory and Arakelov theory play important roles in algebraic geometry and number theory. Indeed, some of the deepest results and conjectures, such as Faltings's proof of Mordell's Conjecture, and the work of Gross and Zagier on the Birch and Swinnerton-Dyer Conjecture, highlight these roles. Deep information typically follows from the derivation of explicit intersection formulae. For example, consider the Gross-Zagier formula [GZ2] and its generalization by Shou-Wu Zhang [Zh1], [Zh2], [Zh3]. We also have recent work on an arithmetic Siegel-Weil formula by Kudla, Rapoport, and the author [Ku1], [KRY1], [KRY2], along with work of Bruinier, Burgos-Gil, and Kühn on an arithmetic Hirzebruch-Zagier formula [BBK]. There are many other famous examples of explicit intersection formulae. There is the work of Gross and Zagier on singular moduli [GZ1], the work of Gross and Keating on modular polynomials [GK], along with its many applications (for example, see [Ku1], [KR1], [KR2]), as well as the recent results of Kudla and Rapoport [KR1, KR2] in the context of Hilbert modular surfaces and Siegel modular 3-folds.

In all of these works, the intersecting cycles are symmetric and are of similar type. We investigate two *different types* of cycles in a Hilbert modular surface defined over \mathbb{Z} : arithmetic Hirzebruch-Zagier divisors, and arithmetic CM cycles associated to non-biquadratic quartic CM fields. These cycles intersect properly, and in earlier work with Bruinier [BY], we conjectured the corresponding arithmetic intersection formula. The truth of this formula has applications to a well known conjecture of Colmez which aims to generalize the classical Chowla-Selberg formula [Co], as well as a conjecture of Lauter on the denominators of the evaluations of Igusa invariants at CM points [La]. Here we prove a special case of the conjectured formula, and as a consequence we obtain the first generalization of the Chowla-Selberg formula to *non-abelian CM number fields*. This result

2000 *Mathematics Subject Classification.* 11G15, 11F41, 14K22.

Partially supported by NSF grants DMS-0302043, 0354353, and a Chinese NSF grant NSFC-10628103.

confirms Colmez's conjecture in this case. It also confirms Lauter's conjecture in certain cases, but for brevity we shall omit a detailed discussion.

We begin by fixing notation. Let $D \equiv 1 \pmod{4}$ be prime, and let $F = \mathbb{Q}(\sqrt{D})$ with the ring of integers $\mathcal{O}_F = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$ and different $\partial_F = \sqrt{D}\mathcal{O}_F$. Let \mathcal{M} be the Hilbert moduli stack over \mathbb{Z} representing the moduli problem that assigns a base scheme S over \mathbb{Z} to the set of the triples (A, ι, λ) , where ([Go, Chapter 3] and [Vo, Section 3])

- (1) A is an abelian surface over S .
- (2) $\iota : \mathcal{O}_F \hookrightarrow \text{End}_S(A)$ is real multiplication of \mathcal{O}_F on A .
- (3) $\lambda : \partial_F^{-1} \rightarrow P(A) = \text{Hom}_{\mathcal{O}_F}(A, A^\vee)^{\text{sym}}$ is a ∂_F^{-1} -polarization (in the sense of Deligne-Papas) satisfying the condition:

$$(1.1) \quad \partial_F^{-1} \otimes A \rightarrow A^\vee, \quad r \otimes a \mapsto \lambda(r)(a)$$

is an isomorphism (of Abelian schemes).

Next, for an integer $m \geq 1$, let \mathcal{T}_m be the integral Hirzebruch-Zagier divisors in \mathcal{M} defined in [BBK, Section 5], which is the flat closure of the classical Hirzebruch-Zagier divisor T_m in \mathcal{M} . For $m = 1$, \mathcal{T}_1 has the following simple moduli description. Let \mathcal{E} be the moduli stack over \mathbb{Z} of elliptic curves, then $E \mapsto (E \otimes \mathcal{O}_F, \iota, \lambda)$ is a closed immersion from \mathcal{E} into \mathcal{M} , and its image is \mathcal{T}_1 .

$$\iota : \mathcal{O}_F \hookrightarrow \text{End}_S(E) \otimes \mathcal{O}_F = \text{End}_{S \otimes \mathcal{O}_F}(E \otimes \mathcal{O}_F) \hookrightarrow \text{End}_S(E \otimes \mathcal{O}_F)$$

is the natural embedding, and

$$\lambda : \partial_F^{-1} \rightarrow \text{Hom}_{S \otimes \mathcal{O}_F}(E \otimes \mathcal{O}_F, E \otimes \partial_F^{-1})^{\text{sym}}, \quad \lambda(z)(e \otimes x) = e \otimes xz.$$

By abuse of notation, we will identify \mathcal{E} with \mathcal{T}_1 .

Finally, let $K = F(\sqrt{\Delta})$ be a quartic non-biquadratic CM number field with real quadratic subfield F . Let $\mathcal{CM}(K)$ be the moduli stack over \mathbb{Z} representing the moduli problem which assigns a base scheme S to the set of the triples (A, ι, λ) where $\iota : \mathcal{O}_K \hookrightarrow \text{End}_S(A)$ is an CM action of \mathcal{O}_K on A , and $(A, \iota|_{\mathcal{O}_F}, \lambda) \in \mathcal{M}(S)$ such that the Rosati involution associated to λ induces to the complex conjugation of \mathcal{O}_K . The map $(A, \iota, \lambda) \mapsto (A, \iota|_{\mathcal{O}_F}, \lambda)$ is a finite proper map from $\mathcal{CM}(K)$ into \mathcal{M} , and we denote its direct image in \mathcal{M} still by $\mathcal{CM}(K)$ by abuse of notation. Since K is non-biquadratic, \mathcal{T}_m and $\mathcal{CM}(K)$ intersect properly. A basic question is to compute their arithmetic intersection number (see Section 2 for definition). We have the following conjectured intersection formula, first stated in [BY]. To state the conjecture, let Φ be a CM type of K and let \tilde{K} be reflex field of (K, Φ) . It is also a quartic non-biquadratic CM field with real quadratic field $\tilde{F} = \mathbb{Q}(\sqrt{\tilde{D}})$ with $\tilde{D} = \Delta\Delta'$. Here Δ' is the Galois conjugate of Δ in F .

Conjecture 1.1. (*Bruinier and Yang [BY]*) *Let the notation be as above. Then*

$$(1.2) \quad \mathcal{T}_m \cdot \mathcal{CM}(K) = \frac{1}{2}b_m$$

or equivalently

$$(1.3) \quad (\mathcal{T}_m \cdot \mathcal{CM}(K))_p = \frac{1}{2}b_m(p)$$

for every prime p . Here

$$b_m = \sum_p b_m(p) \log p$$

is defined as follows:

$$(1.4) \quad b_m(p) \log p = \sum_{\mathfrak{p}|p} \sum_{t=\frac{n+m\sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1}, |n| < m\sqrt{\tilde{D}}} B_t(\mathfrak{p})$$

where

$$(1.5) \quad B_t(\mathfrak{p}) = \begin{cases} 0 & \text{if } \mathfrak{p} \text{ is split in } \tilde{K}, \\ (\text{ord}_{\mathfrak{p}} t_n + 1) \rho(td_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) \log |\mathfrak{p}| & \text{if } \mathfrak{p} \text{ is not split in } \tilde{K}, \end{cases}$$

and

$$\rho(\mathfrak{a}) = \#\{\mathfrak{A} \subset \mathcal{O}_{\tilde{K}} : N_{\tilde{K}/\tilde{F}} \mathfrak{A} = \mathfrak{a}\}.$$

Notice that the conjecture implies that $\mathcal{T}_m \mathcal{CM}(K) = 0$ unless $4Dp|m^2\tilde{D} - n^2$ for some integer $0 \leq n < m\sqrt{\tilde{D}}$, in particular one has to have $p \leq \frac{m^2\tilde{D}}{4D}$.

Throughout this paper, we assume that K satisfies the following condition—we call it condition (\clubsuit):

$$(1.6) \quad \mathcal{O}_K = \mathcal{O}_F + \mathcal{O}_F \frac{w + \sqrt{\Delta}}{2}$$

is free over \mathcal{O}_F and that $\tilde{D} = \Delta\Delta' \equiv 1 \pmod{4}$ is square free ($w \in \mathcal{O}_F$). Under this assumption, one can show that $d_K = D^2\tilde{D}$, and $d_{\tilde{K}} = \tilde{D}^2D$, and $Nd_{\tilde{K}/\tilde{F}} = D$. Here d_K is the discriminant of K , and $d_{\tilde{K}/\tilde{F}}$ is the relative discriminant of \tilde{K}/\tilde{F} . The main purpose of this paper is to prove the conjecture when $m = 1$, and to give a simple procedure for computing $b_1(p)$.

Theorem 1.2. *Under the condition (\clubsuit), Conjecture 1.1 holds for $m = 1$.*

We prove the theorem by computing the local intersection $(\mathcal{CM}(K).T)_p$ and $b_1(p)$ at given p separately and comparing them. On the geometric side, to a geometric intersection point $\iota : \mathcal{O}_K \hookrightarrow \text{End}(E) \otimes \mathcal{O}_F$ we first associate a positive integer n , a sign $\mu = \pm 1$, and a 2×2 integral matrix $T(\mu n)$ with $\det T(\mu n) = \frac{\tilde{D}-n^2}{D} \in 4p\mathbb{Z}_{>0}$ (Proposition 4.3). Next, we use Gross and Keating's beautiful formula [GK] to show the local intersection index at the geometric point ι is equal to $\frac{1}{2}(\text{ord}_p \frac{\tilde{D}-n^2}{4D} + 1)$, depending only on $T(\mu n)$, not on the geometric point itself (Theorem 4.5). Practically, the local intersection index ι is the largest integer m this action can be lifted to W/p^m where W is the Witt ring of $\bar{\mathbb{F}}_p$. The independence on the geometric points is essential and leads us to a simpler problem of counting the number of geometric points $\iota : \mathcal{O}_K \hookrightarrow \text{End}(E) \otimes \mathcal{O}_F$ whose associated matrices is $T(\mu n)$, which is a local density problem representing $T(\mu n)$ by a ternary integral lattice. Explicit computation for the local density problem is given in [Ya1] and [Ya2], but the formula at $p = 2$ is extremely complicated in general. We circumvent it in this special case

by switching it to similar local density problem with clean known answer in Section 5, and obtain the following intersection formula.

Theorem 1.3. *Let the notation and assumption be as in Theorem 1.2, and let p be a prime number. Then*

$$(1.7) \quad (\mathcal{T}_1 \mathcal{CM}(K))_p = \frac{1}{2} \sum_{0 < n < \sqrt{\tilde{D}}, \frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D}-n^2}{4D} + 1) \sum_{\mu} \beta(p, \mu n),$$

where

$$\beta(p, \mu n) = \prod_{\mathfrak{l} \mid \frac{\tilde{D}-n^2}{4D}} \beta_{\mathfrak{l}}(p, \mu n)$$

is given as follows. Given a positive integer $0 < n < \sqrt{\tilde{D}}$ with $\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$ as in (1.7), there is one sign $\mu = \pm 1$ (both signs if $D \mid n$) and a unique positive definite integral 2×2 matrix $T(\mu n)$ satisfying the conditions in Lemma 4.1. For a fixed prime l , $T(\mu n)$ is $\text{GL}_2(\mathbb{Z}_l)$ -equivalent to $\text{diag}(\alpha_l, \alpha_l^{-1} \det T(\mu n))$ with $\alpha_l \in \mathbb{Z}_l^*$. Let $t_l = \text{ord}_l \frac{\tilde{D}-n^2}{4D} = \text{ord}_l T(\mu n) - 2 \text{ord}_l 2$. Then

$$\beta_{\mathfrak{l}}(p, \mu n) = \begin{cases} \frac{1 - (-\alpha_p, p)_p^{t_p}}{2} & \text{if } l = p, \\ \frac{1 + (-1)^{t_l}}{2} & \text{if } l \neq p, (-\alpha_l, l)_l = -1, \\ t_l + 1 & \text{if } l \neq p, (-\alpha_l, l)_l = 1. \end{cases}$$

The theorem has the following interesting consequence.

Corollary 1.4. *Assume (\clubsuit) and $\tilde{D} < 8D$. Then $\mathcal{T}_1 \mathcal{CM}(K) = 0$, i.e., there is no elliptic curve E such that $E \otimes \mathcal{O}_F$ has CM by \mathcal{O}_K .*

In Section 6, we compute $b_1(p)$ and show that it equals twice the right hand side of (1.7) and thus prove Theorem 1.2. From the definition, it is sufficient to prove an identity for each positive integer n with $\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$. After some preparation, one sees that the key is to relate whether \tilde{K}/\tilde{F} is split or inert at a prime \mathfrak{l} to the local property of $T(\mu n)$ at prime $l = \mathfrak{l} \cap \mathbb{Z}$. We prove this unexpected connection in Lemma 6.2, and finish the computation of $b_1(p)$ in Theorem 6.3.

It is worth noting a mysterious identity underlining the conjecture. On the one hand, it is clear from our proof and a general program of Kudla [Ku2] that the intersection number is summation over some Fourier coefficients of the central derivative of some incoherent Siegel-Eisenstein series of genus 3. On the other hand, it is clear from [BY] that $b_m(p)$ comes from summation of certain Fourier coefficients of the central derivative of incoherent Eisenstein series on Hilbert modular surface. Viewing this identity as an identity relating the two seemingly unrelated Eisenstein series, one can naturally ask whether it is a pure accident, or there is some hidden gem?

Now we briefly describe an application of Theorem 1.2 to a conjecture of Colmez, which is a beautiful generalization of the celebrated Chowla-Selberg formula. In proving the famous Mordell conjecture, Faltings introduces the so-called Faltings height $h_{\text{Fal}}(A)$ of an

Abelian variety A , measuring the complexity of A as a point in a Siegel modular variety. When A has complex multiplication, it only depends on the CM type of A and has a simple description as follows. Assume that A is defined over a number field L with good reduction everywhere, and let $\omega_A \in \Lambda^g \Omega_A$ be a Neron differential of A over \mathcal{O}_L , non-vanishing everywhere. Then the Faltings' height of A is defined as (our normalization is slightly different from that of [Co])

$$(1.8) \quad h_{\text{Fal}}(A) = -\frac{1}{2[L : \mathbb{Q}]} \sum_{\sigma: L \hookrightarrow \mathbb{C}} \log \left| \left(\frac{1}{2\pi i} \right)^g \int_{\sigma(A)(\mathbb{C})} \sigma(\omega_A) \wedge \overline{\sigma(\omega_A)} \right| + \log \# \Lambda^g \Omega_A / \mathcal{O}_L \omega_A.$$

Here $g = \dim A$. Colmez gives a beautiful conjectural formula to compute the Faltings height of a CM abelian variety in terms of the log derivative of certain Artin L-series associated to the CM type [Co], which is consequence of his product formula conjecture of p -adic periods in the same paper. When A is a CM elliptic curve, the height conjecture is a reformulation of the well-known Chowla-Selberg formula relating the CM values of the usual Delta function Δ with the values of the Gamma function at rational numbers. Colmez proved his conjecture up to a multiple of $\log 2$ when the CM field (which acts on A) is abelian, refining Gross's [Gr] and Anderson's [Ad] work. A key point is that such CM abelian varieties are quotients of the Jacobians of the Fermat curves, so one has a model to work with. When the CM number field is non-abelian, nothing is known. Conjecture 1.1, together with [BY, Theorem 1.4], would prove Colmez's conjecture for non-biquadratic quartic CM fields, confirming the first *non-abelian* case. More precisely, let K be a non-biquadratic CM number field with totally real quadratic subfield $F = \mathbb{Q}(\sqrt{D})$. Let χ be the quadratic Hecke character of F associated to K/F by the global class field theory, and let

$$(1.9) \quad \Lambda(s, \chi) = C(\chi)^{\frac{s}{2}} \pi^{-s-1} \Gamma\left(\frac{s+1}{2}\right)^2 L(s, \chi)$$

be the complete L-function of χ with $C(\chi) = DN_{F/\mathbb{Q}} d_{K/F}$. Let

$$(1.10) \quad \beta(K/F) = \frac{\Gamma'(1)}{\Gamma(1)} - \frac{\Lambda'(0, \chi)}{\Lambda(0, \chi)} - \log 4\pi.$$

In this case, the conjectured formula of Colmez on the Faltings's height of a CM abelian variety A of type (K, Φ) does not even depend on the CM type Φ and is given by (see [Ya3])

$$(1.11) \quad h_{\text{Fal}}(A) = \frac{1}{2} \beta(K/F).$$

In Section 7, we will prove using Theorem 1.2, and [BY, Theorem 1.4].

Theorem 1.5. *Let K be a non-biquadratic CM quartic CM field of discriminant $D^2 \tilde{D}$ with $D = 5, 13$, or 17 , and $\tilde{D} \equiv 1 \pmod{4}$ prime. Then Colmez's conjecture (1.11) holds.*

Theorem 1.2 also has implications for Lauter's conjecture on the denominator of Igusa invariants at CM points and bad reduction of CM genus two curves in the special cases $D = 5, 13$, and 17 . To keep this paper short, concise, and to the point, we omit this application and refer the reader to [Ya4] for this application, where we prove Conjecture

1.1 under the condition (1.6) and that $\tilde{D} \equiv 1 \pmod{4}$ is a prime. The idea is to prove a weaker version of the conjecture for \mathcal{T}_q when q is a prime split in $F = \mathbb{Q}(\sqrt{D})$ (up to a multiple of $\log q$), and then combining it with [BY, Theorem 1.4] and [BBK, Theorem 4.15] to derive the general case. Although the proof of the weaker version is similar to the case $m = 1$ in this paper in principle, the argument is much more complicated and needs new ideas. The first difficulty is that instead of simple $\text{End}_{\mathcal{O}_F}(E \otimes \mathcal{O}_F) = \text{End}(E) \otimes \mathcal{O}_F$, $\text{End}_{\mathcal{O}_F}(A)$ does not have a good global interpretation. So we have to work locally in terms of Tate modules and Dieudonne modules. Second, the local density problem is no longer a problem representing one matrix by a lattice. Instead, it is really a local Whittaker integral. We have to use a totally different method to compute the local integral.

Here is the organization of this paper. In Section 2, we give basic definition for arithmetic intersection and Faltings' heights in stacks, following [KRY2]. We also show that \mathcal{T}_1 is isomorphic to the stack of elliptic curves. In Section 3, we briefly sketch a proof of Theorem 1.2 in the degenerate case $D = 1$, which is also a new proof of the Gross-Zagier formula on factorization of singular moduli [GZ1]. In Section 4, we use a beautiful formula of Gross and Keating [GK] to compute the local intersection index of \mathcal{T}_1 and $\mathcal{CM}(K)$ at a geometric intersection point. In Section 5, we count the number of geometric intersection points of \mathcal{T}_1 and $\mathcal{CM}(K)$ and prove Theorem 1.3. In Section 6, we compute $b_1(p)$ and finish the proof of Theorem 1.2. In the last section, we prove Theorem 1.5.

Acknowledgement: The author thanks Bruinier, Kudla, Kühn, Lauter, Olsson, Ono, Rapoport, Ribet, and Shou-Wu Zhang for their help during the preparation of this paper. He thanks the referee for his/her careful reading of this paper and very helpful suggestions which makes the exposition of this paper much better. Part of the work was done when the author visited the Max-Planck Institut of Mathematik at Bonn, MSRI, the AMSS and the Morningside Center of Mathematics at Beijing. He thanks these institutes for providing him wonderful working environment.

2. BASIC DEFINITIONS

We basically follow [KRY2, Chapter 2] in our definition of arithmetic intersection and Faltings' height on DM-stacks which have a quotient presentation.

Let \mathcal{M} be a regular DM-stack of dimension n which is proper and flat over \mathbb{Z} . Two cycles \mathcal{Z}_1 and \mathcal{Z}_2 in \mathcal{M} of co-dimensions p and q respectively with $p + q = n$ intersect properly if $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \mathcal{Z}_1 \times_{\mathcal{M}} \mathcal{Z}_2$ is a DM-stack of dimension 0. In this case, we define the (arithmetic) intersection number as

$$(2.1) \quad \mathcal{Z}_1 \cdot \mathcal{Z}_2 = \sum_p \sum_{x \in \mathcal{Z}_1 \cap \mathcal{Z}_2(\mathbb{F}_p)} \frac{1}{\#\text{Aut}(x)} \log \# \tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x} = \sum_p \sum_{x \in \mathcal{Z}_1 \cap \mathcal{Z}_2(\mathbb{F}_p)} \frac{1}{\#\text{Aut}(x)} i_p(\mathcal{Z}_1, \mathcal{Z}_2, x) \log p$$

where $\tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x}$ is the strictly local henselian ring of $\mathcal{Z}_1 \cap \mathcal{Z}_2$ at x ,

$$i_p(\mathcal{Z}_1, \mathcal{Z}_2, x) = \text{Length } \tilde{\mathcal{O}}_{\mathcal{Z}_1 \cap \mathcal{Z}_2, x}$$

is the local intersection index of \mathcal{Z}_1 and \mathcal{Z}_2 at x . If $\phi : \mathcal{Z} \rightarrow \mathcal{M}$ is a finite proper and flat map from stack \mathcal{Z} to \mathcal{M} , we will identify \mathcal{Z} with its direct image $\phi_* \mathcal{Z}$ as a cycle of \mathcal{M} , by abuse of notation.

Now we further assume that its generic fiber $M = \mathcal{M}_{\mathbb{C}} = [\Gamma \backslash X]$ is a quotient stack of a regular proper scheme X , where Γ is a finite group acting on X . Let

$$\text{pr} : X \rightarrow M$$

be the natural projection. We define the arithmetic Picard group $\widehat{\text{Pic}}(\mathcal{M})$ and the arithmetic Chow group $\widehat{\text{CH}}^1(\mathcal{M})$ as in [KRY2, Chapter 2]. For example, let $\hat{Z}^1(\mathcal{M})$ is \mathbb{R} -vector space generated by (\mathcal{Z}, g) , where \mathcal{Z} is a prime divisor in \mathcal{M} (a closed irreducible reduced substack of codimension 1 in \mathcal{M} which is locally in étale topology by a Cartier divisor), and g is a Green function for $Z = \mathcal{Z}(\mathbb{C})$. It means the following. Let $\tilde{Z} = \text{pr}^{-1}(Z)$ be the associated divisor in X . Then the Dirac current δ_Z on M is given by

$$\langle \delta_Z, f \rangle_M = \frac{1}{\#\Gamma} \langle \delta_{\tilde{Z}}, f \rangle_X$$

for every C^∞ function on M with compact support (i.e., every Γ -invariant C^∞ function on X with compact support). A Green function for Z is defined to be a Γ -invariant function g for \tilde{Z} . In such a case, we also have naturally

$$dd^c g + \delta_Z = [\omega]$$

as currents in M for some smooth $(1, 1)$ -form ω on M —a Γ -invariant smooth $(1, 1)$ -form on X (see [KRY2, (2.3.11)]). Although $n = 1$ is assumed in [KRY2], the same argument holds for all n . For a rational function $f \in Q(\mathcal{M})^*$, one defines

$$\widehat{\text{div}}(f) = (\text{div } f, -\log |f|^2) \in \hat{Z}^1(\mathcal{M})$$

Then $\widehat{\text{CH}}^1(\mathcal{M})$ is the quotient space of $\hat{Z}^1(\mathcal{M})$ by the \mathbb{R} -vector space generated by $\widehat{\text{div}}(f)$.

There is a natural isomorphism

$$\widehat{\text{Pic}}(\mathcal{M}) \cong \widehat{\text{CH}}^1(\mathcal{M}),$$

which is induced by $\hat{\mathcal{L}} = (\mathcal{L}, \|\cdot\|) \mapsto (\text{div } s, -\log \|s\|^2)$, s is a rational section of \mathcal{L} . Given a finite proper and flat map $\phi : \mathcal{Z} \rightarrow \mathcal{M}$, it induces a pull-back map ϕ^* from $\widehat{\text{CH}}^1(\mathcal{M})$ to $\widehat{\text{CH}}^1(\mathcal{Z})$, and from $\widehat{\text{Pic}}(\mathcal{M})$ to $\widehat{\text{Pic}}(\mathcal{Z})$. When \mathcal{Z} is a prime cycle of dimension 1 (codimension $n - 1$), and $\hat{\mathcal{L}}$ is a metrized line bundle on \mathcal{M} , we define the Faltings height

$$(2.2) \quad h_{\hat{\mathcal{L}}}(\mathcal{Z}) = \widehat{\text{deg}}(\phi^* \hat{\mathcal{L}})$$

where ϕ is the natural embedding of \mathcal{Z} to \mathcal{M} . Here the arithmetic degree on $\widehat{\text{Pic}}(\mathcal{Z})$ is defined as in [KRY2, (2.18) and (2.19)]. In particular, if s is a (rational) section of \mathcal{L} such that $\text{div } s$ intersects properly with \mathcal{Z} , we have

$$(2.3) \quad h_{\hat{\mathcal{L}}}(\mathcal{Z}) = \mathcal{Z} \cdot \text{div } s - \sum_{z \in Z} \frac{1}{\#\text{Aut}(z)} \log \|s(z)\|$$

where $Z = \mathcal{Z}(\mathbb{C})$. Equivalently, in terms of arithmetic divisors,

$$(2.4) \quad h_{(\mathcal{Z}_1, g_1)}(\mathcal{Z}) = \mathcal{Z}_1 \cdot \mathcal{Z} + \frac{1}{2} \sum_{z \in Z} \frac{1}{\# \text{Aut}(z)} g_1(z), \quad (\mathcal{Z}_1, g_1) \in \widehat{\text{CH}}^1(\mathcal{M})$$

if \mathcal{Z}_1 and \mathcal{Z} intersect properly. The Faltings height is a bilinear map on $\widehat{\text{CH}}^1(\mathcal{M}) \times Z^{n-1}(\mathcal{M})$, which does not factor through $\text{CH}^{n-1}(\mathcal{M})$.

Now come back to our specific case. Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field with $D \equiv 1 \pmod{4}$ being prime. Let \mathcal{M} be the Hilbert modular stack over \mathbb{Z} defined in the introduction. It is regular and flat over \mathbb{Z} but not proper ([DP]). Let $\tilde{\mathcal{M}}$ be a fixed Toroidal compactification of \mathcal{M} , then $\tilde{\mathcal{M}}_{\mathbb{C}}$ and $\mathcal{M}_{\mathbb{C}}$ have quotient presentation (e.g., $\mathcal{M}(\mathbb{C}) = [\Gamma \backslash Y(N)]$ with $Y(N) = \Gamma(N) \backslash \mathbb{H}^2$, and $\Gamma = \Gamma(N) \backslash \text{SL}_2(\mathcal{O}_F)$ for $N \geq 3$). Let $K = F(\sqrt{\Delta})$ be a non-biquadratic quartic CM number field with real quadratic subfield F , and let $\mathcal{CM}(K)$ be the CM cycle defined in the introduction. Notice that $\mathcal{CM}(K)$ is closed in $\tilde{\mathcal{M}}$. K has four different CM types $\Phi_1, \Phi_2, \rho\Phi_1 = \{\rho\sigma : \sigma \in \Phi_1\}$, and $\rho\Phi_2$, where ρ is the complex conjugation in \mathbb{C} . If $x = (A, \iota, \lambda) \in \mathcal{CM}(K)(\mathbb{C})$, then (A, ι, λ) is a CM abelian surface over \mathbb{C} of exactly one CM type Φ_i in $\mathcal{M}(\mathbb{C}) = \text{SL}_2(\mathcal{O}_F) \backslash \mathbb{H}^2$ as defined in [BY, Section 3]. Let $\text{CM}(K, \Phi_i)$ be set of (isomorphism classes) of CM abelian surfaces of CM type (K, Φ_i) as in [BY], viewed as a cycle in $\mathcal{M}(\mathbb{C})$. Then it was proved in [BY]

$$\text{CM}(K) = \text{CM}(K, \Phi_1) + \text{CM}(K, \Phi_2) = \text{CM}(K, \rho\Phi_1) + \text{CM}(K, \rho\Phi_2)$$

is defined over \mathbb{Q} . So we have

Lemma 2.1. *One has*

$$\mathcal{CM}(K)(\mathbb{C}) = 2 \text{CM}(K)$$

in $\mathcal{M}(\mathbb{C})$.

Next, recall that the Hirzebruch-Zagier divisor T_m is given by [HZ]

$$T_m(\mathbb{C}) = \text{SL}_2(\mathcal{O}_F) \backslash \{(z_1, z_2) \in \mathbb{H}^2 : (z_2, 1)A \begin{pmatrix} z_1 \\ 1 \end{pmatrix} = 0 \text{ for some } A \in L_m\},$$

where

$$L_m = \{A = \begin{pmatrix} a & \lambda \\ \lambda' & b \end{pmatrix} : a, b \in \mathbb{Z}, \lambda \in \partial_F^{-1}, ab - \lambda\lambda' = \frac{m}{D}\}.$$

T_m is empty if $(\frac{D}{m}) = -1$. Otherwise, it is a finite union of irreducible curves and is actually defined over \mathbb{Q} . In particular, $T_1(\mathbb{C})$ is the diagonal image of modular curve $\text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ in $\mathcal{M}(\mathbb{C})$. Following [BBK], let \mathcal{T}_m be the flat closure of T_m in \mathcal{M} .

Lemma 2.2. *Let \mathcal{E} be the moduli stack over \mathbb{Z} of elliptic curves. Let $\phi : \mathcal{E} \rightarrow \mathcal{M}$ be given by $\phi(E) = (E \otimes \mathcal{O}_F, \iota_F, \lambda_F)$ for any elliptic curve over a base scheme S , where*

$$\iota_F : \mathcal{O}_F \hookrightarrow \text{End}_S(E) \otimes \mathcal{O}_F = \text{End}_{\mathcal{O}_S \otimes \mathcal{O}_F}(A) \subset \text{End}_S(A)$$

is the natural embedding, and

$$\lambda_F : \partial_F^{-1} \rightarrow \text{Hom}_{\mathcal{O}_E}(E \otimes \mathcal{O}_F, E \otimes \partial_F^{-1})^{\text{sym}}, \quad \lambda_F(z)(e \otimes x) = e \otimes xz.$$

Then ϕ is a closed immersion and $\phi(\mathcal{E}) = \mathcal{T}_1$.

Proof. It is known [BBK, Proposition 5.14] that ϕ is a proper map and its image is \mathcal{T}_1 . To show it is a closed immersion as stacks, it is enough to show

$$\mathrm{Isom}(E, E') \cong \mathrm{Isom}(\phi(E), \phi(E')), \quad f \mapsto \phi(f).$$

Clearly, if $f : E \rightarrow E'$ is an isomorphism, $\phi(f)$ is an isomorphism between $\phi(E)$ and $\phi(E')$. On the other hand, if $g : \phi(E) \rightarrow \phi(E')$ is an isomorphism, i.e., $g : E \otimes \mathcal{O}_F \rightarrow E' \otimes \mathcal{O}_F$ is an \mathcal{O}_F -isomorphism such that

$$(2.5) \quad g^\vee \circ \lambda_F(r) \circ g = \lambda_F(r)$$

for any $r \in \partial_F^{-1}$. Taking a \mathbb{Z} -basis $\{1, \frac{1+\sqrt{D}}{2}\}$ of \mathcal{O}_F , we see $E' \otimes_{\mathbb{Z}} \mathcal{O}_F = (E' \otimes 1) \oplus (E' \otimes \frac{1+\sqrt{D}}{2})$, and that g is uniquely determined by (for any $e \in E$ and $x \in \mathcal{O}_F$)

$$g(e \otimes x) = \alpha(e) \otimes x + \beta(e) \otimes \frac{1 + \sqrt{D}}{2} x$$

for some $\alpha(e), \beta(e) \in E'$, which is determined by g . This implies that α and β are homomorphisms from E to E' . Let α^\vee, β^\vee , and g^\vee be dual maps of α, β , and g , then (for any $e' \in E'$ and $y \in \partial_F^{-1} = (\mathcal{O}_F)^\vee = \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}_F, \mathbb{Z})$)

$$g^\vee(e' \otimes y) = \alpha^\vee(e') \otimes y + \beta^\vee \frac{1 + \sqrt{D}}{2} y.$$

Here we used the simple fact that with respect to the bilinear form on F , $(x, y) = \mathrm{tr} xy$, the dual of an ideal \mathfrak{a} is $\mathfrak{a}^{-1} \partial_F^{-1}$, and the left multiplication $l(r)$ is self-dual: $l(r)^\vee = l(r)$.

Taking $r = 1$, and $x = 1$, we have then for any $e \in E$

$$\begin{aligned} e \otimes 1 &= g^\vee \lambda_F(1) g(e \otimes 1) \\ &= g^\vee(\alpha(e) \otimes 1 + \beta(e) \otimes \frac{1 + \sqrt{D}}{2}) \\ &= \alpha^\vee \alpha(e) \otimes 1 + \beta^\vee \alpha(e) \otimes \frac{1 + \sqrt{D}}{2} + \alpha^\vee \beta(e) \otimes \frac{1 + \sqrt{D}}{2} + \beta^\vee \beta(e) \otimes \left(\frac{1 + \sqrt{D}}{2}\right)^2 \\ &= (\deg \alpha + \deg \beta \frac{D-1}{4}) e \otimes 1 + (\beta^\vee \alpha(e) + \alpha^\vee \beta(e) + \deg \beta) \otimes \frac{1 + \sqrt{D}}{2}. \end{aligned}$$

This implies

$$1 = \deg \alpha + \deg \beta \frac{D-1}{4}.$$

So $\deg \alpha = 1$ and $\deg \beta = 0$. This means that α is an isomorphism, $\beta = 0$, and $g = \phi(\alpha)$. \square

Let ω be the Hodge bundle on $\tilde{\mathcal{M}}$. Then the rational sections of ω^k can be identified with meromorphic Hilbert modular forms for $\mathrm{SL}_2(\mathcal{O}_F)$ of weight k . We give it the following Petersson metric

$$(2.6) \quad \|F(z_1, z_2)\|_{\mathrm{Pet}} = |F(z_1, z_2)| (16\pi^2 y_1 y_2)^{k/2}$$

for a Hilbert modular form $F(z)$ of weight k . This gives a metrized Hodge bundle $\hat{\omega} = (\omega, \|\cdot\|_{\text{Pet}})$. Strictly speaking, the metric has pre-log singularity along the boundary $\tilde{\mathcal{M}} - \mathcal{M}$, [BBK]. Since our CM cycles never intersect with the boundary, the Faltings' height

$$h_{\hat{\omega}}(\mathcal{CM}(K)) = \widehat{\deg}(\phi^*\hat{\omega})$$

is still well-defined where $\phi : \mathcal{CM}(K) \rightarrow \tilde{\mathcal{M}}$ is the natural map. Indeed $\phi^*\hat{\omega}$ is an honest metrized line bundle on $\mathcal{CM}(K)$ as defined here. Faltings's height for these generalized line bundle is defined in [BBK] (for schemes) which is compatible with our definition when applied to stacks. It is proved in [Ya3] that

$$(2.7) \quad h_{\hat{\omega}}(\mathcal{CM}(K)) = \frac{2\#\mathcal{CM}(K)}{W_K} h_{\text{Fal}}(A)$$

for any CM abelian surface $(A, \iota, \lambda) \in \mathcal{CM}(\mathbb{C})$. This will be used in Section 7 to prove Theorem 1.5.

3. THE DEGENERATE CASE

In this section, we briefly sketch a proof of Theorem 1.3 in the degenerate case $D = 1$ ($F = \mathbb{Q} \oplus \mathbb{Q}$) which is a reformulation of Gross and Zagier's work on singular moduli to illustrate the idea behind the proof of Theorem 1.3. It also gives a new proof of the Gross-Zagier formula on factorization of singular moduli [GZ1, Theorem 1.3]. Let \mathcal{M}_1 be the moduli stack over \mathbb{Z} of elliptic curves, Let $\mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_1$ be the modular stack over \mathbb{Z} of pairs of elliptic curves. In this case, \mathcal{T}_1 is the diagonal embedding of \mathcal{M}_1 into \mathcal{M} . Let $K_i = \mathbb{Q}(\sqrt{d_i})$, $i = 1, 2$, be imaginary quadratic fields with fundamental discriminants $d_i < 0$ and ring of integers $\mathcal{O}_i = \mathbb{Z}[\frac{d_i + \sqrt{d_i}}{2}]$, and let $K = K_1 \oplus K_2$. For simplicity, we assume $d_i \equiv 1 \pmod{4}$ are prime to each other. Let $\mathcal{CM}(K_i)$ be the moduli stack over \mathbb{Z} of CM elliptic curves (E, ι_i) where

$$(3.1) \quad \iota_i : \mathcal{O}_i \subset \mathcal{O}_E = \text{End}(E)$$

such that the main involution in \mathcal{O}_E reduces to the complex multiplication on \mathcal{O}_i . Then $\mathcal{CM}(K) = \mathcal{CM}(K_1) \times \mathcal{CM}(K_2)$ is the 'CM cycle' on \mathcal{M} associated to K . It is easy to see that

$$(3.2) \quad \begin{aligned} \mathcal{T}_1.\mathcal{CM}(K) &= \mathcal{CM}(K_1).\mathcal{CM}(K_2) \quad \text{in } \mathcal{M}_1 \\ &= \sum_{\text{disc}[\tau_i]=d_i} \frac{4}{w_1 w_2} \log |j(\tau_1) - j(\tau_2)| \end{aligned}$$

where $w_i = \#\mathcal{O}_i^*$ and τ_i are Heegner points in $\mathcal{M}_1(\mathbb{C})$ of discriminant d_i . So [GZ1, Theorem 1.3] can be rephrased as

Theorem 3.1. (*Gross-Zagier*) *Let the notation be as above, and let $\tilde{D} = d_1 d_2$. Then for a prime p , one has*

$$(3.3) \quad (\mathcal{T}_1.\mathcal{CM}(K))_p = \frac{1}{2} \sum_{\frac{\tilde{D}-n^2}{4} \in p\mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D}-n^2}{4} + 1) \beta(p, n),$$

where

$$\beta(p, n) = \prod_{l \mid \frac{\tilde{D}-n^2}{4}} \beta_l(p, n)$$

is given by

$$\beta_l(p, n) = \begin{cases} \frac{1-\epsilon(p)^{t_p}}{2} & \text{if } l = p, \\ \frac{1+(-1)^{t_l}}{2} & \text{if } l \neq p, \epsilon(l) = -1, \\ t_l + 1 & \text{if } l \neq p, \epsilon(l) = 1. \end{cases}$$

where $t_l = \text{ord}_l \frac{\tilde{D}-n^2}{4}$, and

$$\epsilon(l) = \begin{cases} \left(\frac{d_1}{l}\right) & \text{if } l \nmid d_1, \\ \left(\frac{d_2}{l}\right) & \text{if } l \nmid d_2 \end{cases}$$

is as in [GZ1].

Proof. (sketch) The proof is a simple application of the Gross-Keating formula [GK]. A geometric point of $\mathcal{T}_1 \cap \mathcal{CM}(K) = \mathcal{T}_1 \times_{\mathcal{M}} \mathcal{CM}(K)$ in $F = \bar{\mathbb{F}}_p$ or \mathbb{C} is given by a triple (E, ι_1, ι_2) , with CM action given by (3.1). Since $(d_1, d_2) = 1$, such a point exists only when $F = \bar{\mathbb{F}}_p$ with p nonsplit in K_i and E is supersingular. Assuming this, \mathcal{O}_E is a maximal order of the unique quaternion algebra \mathbb{B} ramified exactly at p and ∞ . Notice that the reduced norm on \mathbb{B} gives a positive quadratic form on \mathbb{B} , and let $(,)$ be the associated bilinear form. Let $\phi_0 = 1$, $\phi_i = \iota_i(\frac{d_i + \sqrt{d_i}}{2})$, then ι_i is determined by ϕ_i . Let

$$T(\phi_0, \phi_1, \phi_2) = \frac{1}{2}((\phi_i, \phi_j))$$

be the matrix associated to three endomorphisms ϕ_i . Then a simple computation gives

$$(3.4) \quad T(\phi_0, \phi_1, \phi_2) = \begin{pmatrix} 1 & 0 & 0 \\ \frac{d_1}{2} & \frac{1}{2} & 0 \\ \frac{d_2}{2} & 0 & \frac{1}{2} \end{pmatrix} \text{diag}(1, T(n)) \begin{pmatrix} 1 & \frac{d_1}{2} & \frac{d_2}{2} \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$$

with $n = 2(\phi_1, \phi_2) - \tilde{D}$ and

$$(3.5) \quad T(n) = \begin{pmatrix} -d_1 & n \\ n & -d_2 \end{pmatrix}.$$

It is easy to see that $\frac{\tilde{D}-n^2}{4} \in \mathbb{Z}_{>0}$ (since the quadratic form is positive definite). In general, for an integer n with $\frac{\tilde{D}-n^2}{4} \in \mathbb{Z}_{>0}$, let $\tilde{T}(n)$ be the 3×3 matrix defined by the right hand side of (3.4). If $\phi_i \in \mathcal{O}_E$ with $\phi_0 = 1$ satisfies $T(\phi_0, \phi_1, \phi_2) = \tilde{T}(n)$, then $\iota_i(\frac{d_i + \sqrt{d_i}}{2}) = \phi_i$ gives actions of \mathcal{O}_i on E and thus a geometric point (E, ι_1, ι_2) in the intersection. By [GK, Proposition 5.4], the local intersection index $i_p(E, \iota_1, \iota_2)$ of \mathcal{T}_1 and $\mathcal{CM}(K)$ at (E, ι_1, ι_2) depends only on $T(\phi_0, \phi_1, \phi_2)$ and is given by (see Theorem 4.5 and its proof for detail)

$$(3.6) \quad i_p(E, \iota_1, \iota_2) = \frac{1}{2}(\text{ord}_p \frac{\tilde{D} - n^2}{4} + 1).$$

So

$$(\mathcal{T}_1.\mathcal{CM}(K))_p = \frac{\log p}{2} \sum_{\frac{\tilde{D}-n^2}{4} \in \mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D}-n^2}{4} + 1) \sum_{E \text{ s.s.}} \frac{R'(\mathcal{O}_E, \tilde{T}(n))}{\#\mathcal{O}_E^*}$$

with

$$R'(\mathcal{O}_E, \tilde{T}(n)) = \#\{\phi_1, \phi_2 \in \mathcal{O}_E : T(1, \phi_1, \phi_2) = \tilde{T}(n)\}.$$

The summation is over isomorphic classes of all supersingular elliptic curves over $\bar{\mathbb{F}}_p$. Next, notice that for two supersingular elliptic curves E_1 and E_2 , $\text{Hom}(E_1, E_2)$ is a quadratic lattice in \mathbb{B} , and they are in the same genus (as E_i changes). Simple argument together with [GK, Corollary 6.23, Proposition 6.25] (see Section 5 for detail) gives

$$\begin{aligned} \sum_{E \text{ s.s.}} \frac{R'(\mathcal{O}_E, \tilde{T}(n))}{\#\mathcal{O}_E^*} &= \sum_{E \text{ s.s.}} \frac{R(\mathcal{O}_E, \tilde{T}(n))}{\#\mathcal{O}_E^* \#\mathcal{O}_E^*} \\ &= \sum_{E_1, E_2 \text{ s.s.}} \frac{R(\text{Hom}(E_1, E_2), \tilde{T}(n))}{\#\mathcal{O}_{E_1}^* \#\mathcal{O}_{E_2}^*} \\ &= \beta(p, n). \end{aligned}$$

Here

$$R(L, \tilde{T}(n)) = \#\{\phi_1, \phi_2, \phi_3 \in L : T(\phi_1, \phi_2, \phi_3) = \tilde{T}(n)\}$$

is the representation number of representing $\tilde{T}(n)$ by the quadratic lattice L . So

$$(\mathcal{T}_1.\mathcal{CM}(K))_p = \frac{1}{2} \sum_{\frac{\tilde{D}-n^2}{4} \in \mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D}-n^2}{4} + 1) \beta(p, n).$$

Notice that $\beta_p(p, n) = 0$ when $p \nmid \frac{\tilde{D}-n^2}{4}$ by the formula for $\beta_p(p, n)$. So the summation is really over $\frac{\tilde{D}-n^2}{4} \in p\mathbb{Z}_{>0}$. This proves the theorem. \square

In the degenerate case, it is reasonable to view $\tilde{K} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ as the reflex field of $K = \mathbb{Q}(\sqrt{d_1}) \oplus \mathbb{Q}(\sqrt{d_2})$ with respect to the ‘CM type’ $\Phi = \{1, \sigma\}$:

$$\sigma(\sqrt{d_1}, \sqrt{d_2}) = (\sqrt{d_2}, \sqrt{d_1}), \quad \sigma(\sqrt{d_2}, \sqrt{d_1}) = (-\sqrt{d_1}, \sqrt{d_2}).$$

\tilde{K} has real quadratic subfield $\tilde{F} = \mathbb{Q}(\sqrt{\tilde{D}})$ with $\tilde{D} = d_2 d_1$. Using this convention, one can define $b_m(p)$ and b_m as in Conjecture 1.1. We leave it to the reader to check that

$$b_1(p) = \sum_{\frac{\tilde{D}-n^2}{4} \in p\mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D}-n^2}{4} + 1) \beta(p, n),$$

and thus $\mathcal{T}_1.\mathcal{CM}(K) = \frac{1}{2} b_1$. This verifies Conjecture 1.1 for the degenerate case $D = 1$.

4. LOCAL INTERSECTION INDICES

Lemma 4.1. *Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field with $D \equiv 1 \pmod{4}$ prime. Let $\Delta \in \mathcal{O}_F$ be totally negative and let $\tilde{D} = \Delta\Delta'$. Let n be an integer $0 < n < \sqrt{\tilde{D}}$ with $\frac{\tilde{D}-n^2}{D} \in \mathbb{Z}_{>0}$.*

(a) *When $D \nmid n$, there is a unique sign $\mu = \mu(n) = \pm 1$ and a unique positive definite integral matrix $T(\mu n) = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \text{Sym}_2(\mathbb{Z})$ such that*

$$(4.1) \quad \det T(\mu n) = \frac{\tilde{D} - n^2}{D},$$

$$(4.2) \quad \Delta = \frac{2\mu n - Dc - (2b + Dc)\sqrt{D}}{2}.$$

Moreover, one has

$$(4.3) \quad a + Db + \frac{D^2 - D}{4}c = -\mu n.$$

(b) *When $D|n$, for each $\mu = \pm 1$, there is a unique positive definite integral matrix $T(\mu n) = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \text{Sym}_2(\mathbb{Z})$ such that (4.1) and (4.2) hold. In each case, (4.3) holds.*

Proof. Write $\Delta = \frac{u+v\sqrt{D}}{2}$, then $u^2 - v^2D = 4\tilde{D}$, and so

$$u^2 \equiv 4\tilde{D} \pmod{D} \equiv 4n^2 \pmod{D}.$$

This implies $D|(u - 2n)(u + 2n)$.

(a) Since $D \nmid 4n$ is prime, there is thus a unique $\mu = \pm 1$ and unique integer c such that

$$u = 2\mu n - Dc.$$

Since Δ is totally negative, $u < 0$. So $u^2 \geq 4\tilde{D} > 4n^2$, and so $u < 2\mu n$, and $c > 0$. (4.2) also gives $b = \frac{-v-Dc}{2} = \frac{u-v}{2} + \mu n \in \mathbb{Z}$. Next, (4.1) gives a unique $a \in \mathbb{Q}_{>0}$, and $T(\mu n) > 0$. We now verify that a is an integer by showing that it satisfies (4.3). The equation (4.1) gives

$$4Dac - 4Db^2 = 4\tilde{D} - 4n^2 = -v^2D - 2uDc - D^2c^2.$$

So

$$\begin{aligned} 4ac &= -Dc(4b + Dc) - 2(2\mu n - Dc)c - Dc^2 \\ &= -4Dbc - D^2c^2 + Dc^2 - 4\mu n, \end{aligned}$$

and so

$$a + Db + \frac{D^2 - D}{4}c = -\mu n$$

as claimed in (4.3).

(b) When $D|n$, $D|u$. So for each $\mu = \pm 1$, there is a unique integer n such that $u = 2\mu n - Dc$. Everything else is the same as in (a). \square

Remark 4.2. Throughout this paper, the sum \sum_{μ} means either $\sum_{\mu=\pm 1}$ when $D|n$ or the unique term μ satisfying the condition in Lemma 4.1 when $D \nmid n$.

Let E be a supersingular elliptic curve over $k = \bar{\mathbb{F}}_p$. Then $\mathcal{O}_E = \text{End}(E)$ is a maximal order of the unique quaternion algebra \mathbb{B} ramified exactly at p and ∞ . Let

$$(4.4) \quad L_E = \{x \in \mathbb{Z} + 2\mathcal{O}_E : \text{tr } x = 0\}$$

be the so-called Gross lattice with quadratic form $Q(x) = x\bar{x} = -x^2$, where $x \mapsto \bar{x}$ is the main involution of \mathbb{B} . The reduced norm gives a quadratic form on \mathbb{B} . For $x_1, x_2, \dots, x_n \in \mathbb{B}$, we define

$$(4.5) \quad T(x_1, x_2, \dots, x_n) = \frac{1}{2}((x_i, x_j)) \in \text{Sym}_n(\mathbb{Q}).$$

Proposition 4.3. *Let the notation and assumption be as in Theorem 1.2. Let p be a prime and E be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$ with endomorphism ring \mathcal{O}_E . Then there is a one-to-one correspondence among the following three sets.*

- (1) *The set $I(E)$ of ring embeddings $\iota : \mathcal{O}_K \hookrightarrow \text{End}_{\mathcal{O}_F}(E \otimes \mathcal{O}_F) = \mathcal{O}_E \otimes \mathcal{O}_F$ satisfying*
 - (a) *$\iota(a) = 1 \otimes a$ for $a \in \mathcal{O}_F$, and*
 - (b) *the main involution in \mathcal{O}_E induces the complex conjugation on \mathcal{O}_K via ι .*
- (2) *The set $\mathbb{T}(E)$ of $(\delta, \beta) \in L_E^2$ such that $T(\delta, \beta) = T(\mu n)$ for some integer $0 < n < \sqrt{D}$ such that $\frac{D-n^2}{4D} \in p\mathbb{Z}_{>0}$ and a unique $\mu = \pm 1$.*
- (3) *The set $\tilde{\mathbb{T}}(E)$ of $(\alpha_0, \beta_0) \in \mathcal{O}_E^2$ such that $T(1, \alpha_0, \beta_0) = \tilde{T}(\mu n)$ for some integer $0 < n < \sqrt{D}$ such that $\frac{D-n^2}{4D} \in p\mathbb{Z}_{>0}$ and a unique $\mu = \pm 1$. Here*

$$\tilde{T} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{w_0}{2} & \frac{1}{2} & 0 \\ \frac{w_1}{2} & 0 & \frac{1}{2} \end{pmatrix} \text{diag}(1, T) \begin{pmatrix} 1 & \frac{w_1}{2} & \frac{w_1}{2} \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & \frac{w_1}{2} & \frac{w_1}{2} \\ \frac{w_0}{2} & \frac{1}{4}(a + w_0^2) & \frac{1}{4}(b + w_0 w_1) \\ \frac{w_1}{2} & \frac{1}{4}(b + w_0 w_1) & \frac{1}{4}(c + w_1^2) \end{pmatrix}$$

for $T = T(\mu n)$. Here $w = w_0 + w_1 \frac{D+\sqrt{D}}{2}$ is given in (1.6).

The correspondences are determined by

$$(4.6) \quad \iota\left(\frac{w + \sqrt{\Delta}}{2}\right) = \alpha_0 + \beta_0 \frac{D + \sqrt{D}}{2},$$

$$(4.7) \quad \iota(\sqrt{\Delta}) = \delta + \beta \frac{D + \sqrt{D}}{2},$$

$$(4.8) \quad \delta = 2\alpha_0 - w_0, \quad \beta = 2\beta_0 - w_1.$$

Proof. Given an embedding $\iota \in I(E)$, we define $\alpha_0, \beta_0, \delta$ and β by (4.6) and (4.7). They satisfy (4.8), and $(\delta, \beta) \in L_E^2$. Write $T(\delta, \beta) = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ with $a = \frac{1}{2}(\delta, \delta) = -\delta^2$, $b = \frac{1}{2}(\delta, \beta)$, and $c = \frac{1}{2}(\beta, \beta) = -\beta^2$. First,

$$\begin{aligned} \Delta &= \iota(\Delta) = \iota(\sqrt{\Delta})^2 = (\delta + \frac{D}{2}\beta)^2 - (\delta + \frac{D}{2}\beta, \frac{1}{2}\beta)\sqrt{D} \\ &= -a - Db - \frac{D^2 + D}{4}c - (b + \frac{1}{2}Dc)\sqrt{D}. \end{aligned}$$

We define $n > 0$ and $\mu = \pm 1$ by

$$-\mu n = a + Db + \frac{D^2 - D}{4}c.$$

Then

$$\Delta = \frac{2\mu n - Dc - (2b + Dc)\sqrt{D}}{2}$$

satisfying (4.2) in Lemma 4.1. Now a simple calculation using $\tilde{D} = \Delta\Delta'$ gives

$$\det T(\delta, \beta) = ac - b^2 = \frac{\tilde{D} - n^2}{D}$$

satisfies (4.1). So $T(\delta, \beta) = T(\mu n)$ for a unique n satisfying the conditions in Lemma 4.1. To show $p \mid \det T(\mu n)$, let

$$\gamma = (\delta, \beta) + 2\delta\beta \in L_E.$$

Then

$$(\delta, \gamma) = (\beta, \gamma) = 0, \quad (\gamma, \gamma) = 2(\delta, \delta)(\beta, \beta) - 2(\delta, \beta)^2 = 8 \det T(\mu n).$$

So the determinant of $\{\delta, \beta, \gamma\}$ is

$$\det T(\delta, \beta, \gamma) = \det \text{diag}(T(\mu n), 4 \det T(\mu n)) = 4 \det T(\mu n)^2.$$

Since L_E has determinant $4p^2$, we have thus $p \mid \det T(\mu n)$. To show $4 \mid \det T(\mu n)$, it is easier to look at $\tilde{T}(\mu n) \in \text{Sym}_3(\mathbb{Z})^\vee$ (since $\alpha_0, \beta_0 \in \mathcal{O}_E$). It implies that

$$(4.9) \quad a \equiv -w_0^2 \pmod{4}, \quad b \equiv -w_0 w_1 \pmod{2}, \quad c \equiv -w_1^2 \pmod{4}.$$

So $\det T(\mu n) = ac - b^2 \equiv 0 \pmod{4}$, and therefore $(\delta, \beta) \in \mathbb{T}(E)$. A simple linear algebra calculation shows that $(\alpha_0, \beta_0) \in \tilde{\mathbb{T}}(E)$.

Next, we assume that $(\delta, \beta) \in \mathbb{T}(E)$. Define ι and (α_0, β_0) by (4.7) and (4.8). The above calculation gives

$$(\delta + \beta \frac{D + \sqrt{D}}{2})^2 = \Delta,$$

so ι gives an embedding from K into $\mathbb{B} \otimes \mathcal{O}_F$ satisfying the conditions in (1) once we verify $\iota(\mathcal{O}_K) \subset \mathcal{O}_E \otimes \mathcal{O}_F$, which is equivalent to $\alpha_0, \beta_0 \in \mathcal{O}_E$. Write

$$\delta = -u_0 + 2\alpha_1, \quad \beta = -u_1 + 2\beta_1, \quad u = u_0 + u_1 \frac{D + \sqrt{D}}{2}$$

with $u_i \in \mathbb{Z}$, $\alpha_1, \beta_1 \in \mathcal{O}_E$. Then

$$\iota(\frac{u + \sqrt{\Delta}}{2}) = \alpha_1 + \beta_1 \frac{D + \sqrt{D}}{2} \in \mathcal{O}_E \otimes \mathcal{O}_F.$$

This implies that $\frac{u + \sqrt{\Delta}}{2} \in \mathcal{O}_K$. On the other hand, $\frac{w + \sqrt{\Delta}}{2} \in \mathcal{O}_K$. So $\frac{u - w}{2} \in \mathcal{O}_F$, i.e., $\frac{w_i - u_i}{2} \in \mathbb{Z}$, and

$$\alpha_0 = \alpha_1 + \frac{w_0 - u_1}{2} \in \mathcal{O}_E, \quad \beta_0 = \beta_1 + \frac{w_1 - u_1}{2} \in \mathcal{O}_E$$

as claimed. So $(\alpha_0, \beta_0) \in \tilde{\mathbb{T}}(E)$ and $\iota \in I(E)$. Finally, if $(\alpha_0, \beta_0) \in \tilde{\mathbb{T}}(E)$, it is easy to check that $(\delta, \beta) \in \mathbb{T}(E)$. \square

The proof also gives the following interesting fact. In particular, Corollary 1.4 is true.

Corollary 4.4. *Let K be a non-biquadratic quartic CM number field with real quadratic subfield $F = \mathbb{Q}(\sqrt{D})$ where D does not need to be a prime. If \mathcal{O}_K is a free \mathcal{O}_F -module as in (1.6) with $\tilde{D} = \Delta\Delta' < 8D$ (not necessarily square free or odd). There is no elliptic curve E such that $E \otimes \mathcal{O}_F$ has an \mathcal{O}_K -action whose restriction to \mathcal{O}_F coincides with the natural action of \mathcal{O}_F on $E \otimes \mathcal{O}_F$.*

Proof. If such an CM action exists, E has to be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$ for some prime p . Let ι be the resulting embedding $\iota : \mathcal{O}_K \hookrightarrow \mathcal{O}_E \otimes \mathcal{O}_F$. The main involution of \mathbb{B} induces an automorphism of K which is the identity on F . Extending this through one real embedding σ of F , we get an embedding $\iota : \mathbb{C} \hookrightarrow \mathbb{B} \otimes \mathbb{R}$, which is the division quaternion algebra over \mathbb{R} . Then main involution has to induces the complex conjugation of \mathbb{C} and thus K . Now the same argument as above implies that there is an integer $n > 0$ such that $\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{\geq 0}$. Since \tilde{D} is not a square (K is not biquadratic), one has $\frac{\tilde{D}-n^2}{4D} \geq p \geq 2$, i.e., $\tilde{D} \geq 8D$, a contradiction. \square

We are now ready to deal with local intersection indices of \mathcal{T}_1 and $\mathcal{CM}(K)$ at a geometric intersection point. In view of Lemma 2.2, we consider the fiber product

$$(4.10) \quad \begin{array}{ccc} \mathcal{CM}(K) \times_{\mathcal{M}} \mathcal{E} & \xrightarrow{\tilde{f}} & \mathcal{E} \\ \downarrow \tilde{\phi} & & \downarrow \phi \\ \mathcal{CM}(K) & \xrightarrow{f} & \mathcal{M} \end{array}.$$

An element in $\mathcal{CM}(K) \times_{\mathcal{M}} \mathcal{E}(S)$ is a tube (E, A, ι, λ) such that $(A, \iota, \lambda) \in \mathcal{CM}(K)(S)$ $E \in \mathcal{E}(S)$ satisfying

$$A = E \otimes \mathcal{O}_F, \quad \iota|_{\mathcal{O}_F} = \iota_F, \quad \lambda = \lambda_F$$

where ι_F and λ_F are given in Lemma 2.2. This is determined by

$$\iota : \mathcal{O}_K \hookrightarrow \mathcal{O}_E \otimes \mathcal{O}_F$$

with $\iota \in I(E)$. So an intersection point $x = (E \otimes \mathcal{O}_F, \iota_F, \lambda_F) \in \mathcal{CM}(K) \cap \mathcal{T}_1(S)$ is given by a pair (E, ι) with $\iota \in I(E)$. When $S = \text{Spec}(F)$ for an algebraically closed field $F = \mathbb{C}$ or $\bar{\mathbb{F}}_p$, such a pair exists only when $F = \bar{\mathbb{F}}_p$ and E is supersingular. Assuming this, and write $\mathcal{Z} = \mathcal{CM}(K) \cap \mathcal{T}_1$. Let W be the Witt ring of $\bar{\mathbb{F}}_p$, and let \mathbb{E} be the universal lifting of E to $W[[t]]$, and let I be the minimal ideal of $W[[t]]$ such that ι can be lifted to an embedding

$$\iota_I : \mathcal{O}_K \hookrightarrow \text{End}(\mathbb{E} \bmod I) \otimes \mathcal{O}_F.$$

Then the deformation theory implies the strictly local henselian ring $\tilde{\mathcal{O}}_{\mathcal{Z},x}$ is equal to

$$\tilde{\mathcal{O}}_{\mathcal{Z},x} = W[[t]]/I.$$

So

$$(4.11) \quad i_p(\mathcal{CM}(K), \mathcal{T}_1, x) = \text{Length}_W W[[t]]/I,$$

which we also denote by $i_p(E, \iota)$. Therefore

$$(4.12) \quad (\mathcal{CM}(K). \mathcal{T}_1)_p = \sum_{E.s.s., \iota \in I(E)} \frac{1}{\#\mathcal{O}_E^*} i_p(E, \iota) \log p.$$

Here ‘s.s.’ stands for supersingular elliptic curves. Notice that $\text{Aut}(x) = \text{Aut}(E) = \mathcal{O}_E^*$ by Lemma 2.2. The local intersection index $i_p(E, \iota)$ can be computed by a beautiful formula of Gross and Keating [GK] as follows.

Theorem 4.5. *Let the notation be as above, and let $(\delta, \beta) \in \mathbb{T}(E)$ be the image of $\iota \in I(E)$, and let $T(\mu n) = T(\delta, \beta)$ as in Proposition 4.3. Then*

$$i_p(E, \iota) = \frac{1}{2}(\text{ord}_p \frac{\tilde{D} - n^2}{4D} + 1)$$

depends only on n .

Proof. Let $(\alpha_0, \beta_0) \in \tilde{\mathbb{T}}(n)$ be the image of ι . First notice that I is also the smallest ideal of $W[[t]]$ such that α_0 and β_0 can be lifted to endomorphisms of $\mathbb{E} \bmod I$. Applying the Gross-Keating formula [GK, Proposition 5.4] to $f_1 = 1$, $f_2 = \alpha_0$, and $f_3 = \beta_0$, we see that $i_p(K, \iota)$ depends on the $\text{GL}_3(\mathbb{Z}_p)$ -equivalence class of $\tilde{T}(\mu n)$ and is given as follows.

Let $a_0 \leq a_1 \leq a_2$ be the Gross-Keating invariants of the quadratic form

$$(4.13) \quad Q(x + y\alpha_0 + z\beta_0) = (x, y, z)\tilde{T}(\mu n)(x, y, z)^t$$

defined in [GK, Section 4]. Then $i_p(E, \iota)$ equals

$$\begin{aligned} & \sum_{i=0}^{a_0-1} (i+1)(a_0 + a_1 + a_2 - 3i)p^i + \sum_{i=a_0}^{(a_0+a_1-2)/2} (a_0+1)(2a_0 + a_1 + a_2 - 4i)p^i \\ & + \frac{a_0+1}{2}(a_2 - a_1 + 1)p^{\frac{a_0+a_1}{2}} \end{aligned}$$

if $a_1 - a_0$ is even, and

$$\sum_{i=0}^{a_0-1} (i+1)(a_0 + a_1 + a_2 - 3i)p^i + \sum_{i=a_0}^{(a_0+a_1-1)/2} (a_0+1)(2a_0 + a_1 + a_2 - 4i)p^i$$

if $a_1 - a_0$ is odd.

First assume that p is odd. In this case, $\tilde{T}(\mu n)$ is $\text{GL}_3(\mathbb{Z}_p)$ -equivalent to $\text{diag}(1, T(\mu n))$. Notice that $p \nmid T(\mu n)$, $T(\mu n)$ is $\text{GL}_2(\mathbb{Z}_p)$ -equivalent to $\text{diag}(\alpha_p, \alpha_p^{-1} \det T(\mu n))$ for some $\alpha_p \in \mathbb{Z}_p^*$, so $\tilde{T}(\mu n)$ is equivalent to $\text{diag}(1, \alpha_p, \alpha_p^{-1} \det T(\mu n))$. So the Gross-Keating invariants are $(0, 0, \text{ord}_p \det T(\mu n))$ in this case. The Gross-Keating formula gives

$$i_p(E, \iota) = \frac{1}{2}(\text{ord}_p \det T(\mu n) + 1) = \frac{1}{2}(\text{ord}_p \frac{\tilde{D} - n^2}{4D} + 1).$$

Now we assume $p = 2$. Since the quadratic form Q associated to $\tilde{T}(\mu n)$ is anisotropic over \mathbb{Q}_2 , $\tilde{T}(\mu n)$ is $\text{GL}_3(\mathbb{Z}_2)$ -equivalent to either

$$\text{diag}(\epsilon_0 2^{t_0}, 2^s \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}) \quad \text{or} \quad \text{diag}(\epsilon_1 2^{t_1}, \epsilon_2 2^{t_2}, \epsilon_3 2^{t_3})$$

with $\epsilon_i \in \mathbb{Z}_2^*$ and $t_i, s \in \mathbb{Z}_{\geq 0}$. Since $\tilde{T}(\mu n)$ is not integral over \mathbb{Z}_2 (at least one of w_0 or w_1 is odd), $\tilde{T}(\mu n)$ has to be $\text{GL}_3(\mathbb{Z}_2)$ -equivalent to $\text{diag}(\epsilon_0 2^{t_0}, \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix})$. In this case, [Ya2, Proposition B.4] asserts that the Gross-Keating invariants are $(0, 0, t_0)$. Since

$$3\epsilon_0 2^{t_0-2} = \det \tilde{T}(\mu n) = \frac{1}{16} \det T(\mu n) = \frac{1}{4} \frac{\tilde{D} - n^2}{4D},$$

we see $t_0 = \text{ord}_2 \frac{\tilde{D} - n^2}{4D}$. Now the Gross-Keating formula gives the desired formula for $p = 2$. \square

We remark that when $p \neq 2$, the ideal I is also the minimal ideal such that δ and β can be lifted to endomorphisms of $\mathbb{E} \bmod I$. It is not true for $p = 2$. In summary, we have our first main formula.

Theorem 4.6. *Let the notation and assumption be as in Theorem 1.2. Then*

$$\mathcal{CM}(K) \cdot \mathcal{T}_1 = \frac{1}{2} \sum_p \log p \sum_{0 < n < \sqrt{\tilde{D}}, \frac{\tilde{D} - n^2}{4D} \in p\mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D} - n^2}{4D} + 1) \sum_{\mu} \sum_{E \text{ s.s.}} \frac{R(L_E, T(\mu n))}{\#\mathcal{O}_E^*}$$

where $R(L, T)$ is the number of a lattice L representing T , i.e.,

$$R(L, T) = \# \{x = (x_1, x_2) \in L^2 : T(x_1, x_2) = T\}.$$

Here the meaning of \sum_{μ} is given in Remark 4.2.

5. LOCAL DENSITY

It is not hard to prove that the quantity $\sum_{E \text{ s.s.}} \frac{R(L_E, T(\mu n))}{\#\mathcal{O}_E^*}$ is product of the so-called local densities. Explicit formulae for these local densities are given by the author in [Ya1, Propositions 8.6 and 8.7] for $p \neq 2$. When $p = 2$, an algorithm is given in [Ya2] and could be used to get a formula in our case, but it is cumbersome. We give an alternative way to compute it in this section. We first prove

Lemma 5.1. *Let $T \in \text{Sym}_2(\mathbb{Z})$ and let \tilde{T} be obtained from T by the formula in Proposition 4.3(3). Assume $\tilde{T} \in \text{Sym}_3(\mathbb{Z})^\vee$. Then*

$$\sum_{E \text{ s.s.}} \frac{R(L_E, T)}{\#\mathcal{O}_E^*} = \sum_{E, E' \text{ s.s.}} \frac{R(\text{Hom}(E, E'), \tilde{T})}{\#\mathcal{O}_E^* \#\mathcal{O}_{E'}^*}.$$

Here $\text{Hom}(E, E')$ is equipped with the degree as its quadratic form.

Proof. Clearly $T(\delta, \beta) = T$ if and only if $T(1, \alpha_0, \beta_0) = \tilde{T}$ where δ, β, α_0 , and β_0 are related by (4.8). The condition $\tilde{T} \in \text{Sym}_3(\mathbb{Z})^\vee$ implies that $(\delta, \beta) \in L_E^2$ if and only if $(\alpha_0, \beta_0) \in \mathcal{O}_E^2$. Next if $f_1, f_2, f_3 \in \mathcal{O}_E$ represents \tilde{T} , i.e., $T(f_1, f_2, f_3) = \tilde{T}$, then the reduced norm $Nf_1 = 1$, and $f_1 \in \mathcal{O}_E^*$. In such a case, $1, \alpha_0 = f_1^{-1}f_2, \beta_0 = f_1^{-1}f_3$ represents \tilde{T} too. So

$$R(\mathcal{O}_E, \tilde{T}) = \#\mathcal{O}_E^* R(L_E, T)$$

and

$$\sum_{E \text{ s.s.}} \frac{R(L_E, T)}{\#\mathcal{O}_E^*} = \sum_{E \text{ s.s.}} \frac{R(\mathcal{O}_E, \tilde{T})}{(\#\mathcal{O}_E^*)^2}.$$

On the other hand, if $f_1, f_2, f_3 \in \text{Hom}(E, E')$ represents \tilde{T} , then $\deg f_1 = 1$ and f_1 is actually an isomorphism. So $R(\text{Hom}(E, E'), \tilde{T}) = 0$ unless E and E' are isomorphic. This proves the lemma. \square

The quantity

$$\sum_{E, E' \text{ s.s.}} \frac{R(\text{Hom}(E, E'), \tilde{T})}{\#\mathcal{O}_E^* \#\mathcal{O}_{E'}^*}$$

is also a product of local densities and is computed by Gross and Keating [GK, Section 6] in terms of Gross-Keating invariants (see also [We2] and [We1] for more extensive explanation). More precisely, we have (note that $\det Q$ in [GK] is our $\det 2\tilde{T}$),

$$(5.1) \quad \sum_{E, E' \text{ s.s.}} \frac{R(\text{Hom}(E, E'), \tilde{T})}{\#\mathcal{O}_E^* \#\mathcal{O}_{E'}^*} = \prod_{l|4p \det \tilde{T}} \beta_l(\tilde{T}).$$

Here $\beta_p(\tilde{T})$ is 0 or 1 depending on whether \tilde{T} is isotropic or anisotropic over \mathbb{Z}_p . For $l \neq p$, $\beta_l(\tilde{T})$ is zero if \tilde{T} is anisotropic over \mathbb{Z}_l and is given as follows if \tilde{T} is isotropic by [GK, Proposition 6.24]. Let $0 \leq a_0 \leq a_1 \leq a_2$ be Gross-Keating invariants of \tilde{T} , and let $\epsilon = \pm 1$ be the Gross-Keating epsilon sign of \tilde{T} , then

If $a_0 \equiv a_1 \pmod{2}$ and $\epsilon = 1$, we have

$$\beta_l(\tilde{T}) = 2 \sum_{i=0}^{a_0-1} (i+1)l^i + 2 \sum_{i=a_0}^{(a_0+a_1-2)/2} (i+1)l^i + (a_0+1)(a_2-a_1+1)l^{\frac{a_0+a_1}{2}}.$$

If $a_0 \equiv a_1 \pmod{2}$ and $\epsilon = -1$, we have

$$\beta_l(\tilde{T}) = 2 \sum_{i=0}^{a_0-1} (i+1)l^i + 2 \sum_{i=a_0}^{(a_0+a_1-2)/2} (i+1)l^i + (a_0+1)l^{\frac{a_0+a_1}{2}}.$$

If $a_0 \not\equiv a_1 \pmod{2}$, we have

$$\beta_l(\tilde{T}) = 2 \sum_{i=0}^{a_0-1} (i+1)l^i + 2 \sum_{i=a_0}^{(a_0+a_1-1)/2} (i+1)l^i.$$

Lemma 5.2. *Let n be a positive integer such that $\frac{\tilde{D}-n^2}{4D} \in \mathbb{Z}_{>0}$ and let $T(\mu n)$ be as in Lemma 4.1. Then*

- (1) $T(\mu n)$ is $\text{GL}_2(\mathbb{Z})_l$ -equivalent to $\text{diag}(\alpha_l, \alpha_l^{-1} \det T(\mu n))$ for some $\alpha_l \in \mathbb{Z}_l$.
- (2) $\tilde{T}(\mu n)$ is isotropic if and only if $(-\alpha_l, l)_l^{t_l} = 1$ where $t_l = \text{ord}_l \frac{\tilde{D}-n^2}{4D}$.

Proof. (1) follows from the fact $l \nmid a$ or $l \nmid c$. By (1), $\tilde{T}(\mu n)$ is $\mathrm{GL}_3(\mathbb{Q}_l)$ -equivalent to $\mathrm{diag}(1, \alpha_l, \alpha_l^{-1} \det T(\mu n))$. So its Hasse invariant is $(\alpha_l, -\det T(\mu n))_l$. By [Se, Chapter 4, Theorem 6], $\tilde{T}(\mu n)$ is isotropic over \mathbb{Z}_l if and only if

$$(\alpha_l, -\det T(\mu n))_l = (-1, -\det \tilde{T}(\mu n))_l,$$

i.e.,

$$(-\alpha_l, -\frac{\tilde{D} - n^2}{4D})_l = 1.$$

When $l \neq 2$,

$$(-\alpha_l, -\frac{\tilde{D} - n^2}{4D})_l = (-\alpha_l, l)_l^{t_l}.$$

When $l = 2$, Lemma 6.1 in the next section asserts that either $a \equiv -1 \pmod{4}$ or $c \equiv -1 \pmod{4}$. So $\alpha_2 = a$ or c , and thus $-\alpha_2 \equiv 1 \pmod{4}$. This implies

$$(-\alpha_2, -\frac{\tilde{D} - n^2}{4D})_2 = (-\alpha_2, 2)_2^{t_2}.$$

just as in the odd case. □

Proposition 5.3. *Assume that $0 < n < \sqrt{\tilde{D}}$ with $\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$. Then*

$$\sum_{E \text{ s.s.}} \frac{R(L_E, T(\mu n))}{\#\mathcal{O}_E^*} = \prod_{l \mid \frac{\tilde{D}-n^2}{4D}} \beta_l(p, \mu n).$$

Here $\beta_l(p, \mu n)$ is given as follows. Let $T(\mu n)$ be $\mathrm{GL}_2(\mathbb{Z}_l)$ -equivalent to $\mathrm{diag}(\alpha_l, \alpha_l^{-1} \det T(\mu n))$ over \mathbb{Z}_l with $\alpha_l \in \mathbb{Z}_l^*$, and write $t_l = \mathrm{ord}_l \frac{\tilde{D}-n^2}{4D}$. Then

$$\beta_l(p, \mu n) = \begin{cases} \frac{1 - (-\alpha_p, p)_p^{t_p}}{2} & \text{if } l = p, \\ \frac{1 + (-1)^{t_l}}{2} & \text{if } l \neq p, \text{ and } (-\alpha_l, l)_l = -1, \\ t_l + 1 & \text{if } l \neq p, \text{ and } (-\alpha_l, l)_l = 1. \end{cases}$$

Proof. By Lemma 5.1 and (5.1), it suffices to verify the formula for $\beta_l(p, n)$. The case $l = p$ follows from Lemma 5.2.

When $l \nmid 2p$, $\tilde{T}(\mu n)$ is $\mathrm{GL}_3(\mathbb{Z}_l)$ -equivalent to $\mathrm{diag}(1, T)$ and thus to $\mathrm{diag}(1, \alpha_l, \alpha_l^{-1} \det T(\mu n))$. When it is isotropic, its Gross-Keating epsilon sign is $(-\alpha_l, l)_l$ by definition [GK, Section 3]. So its Gross-Keating invariants are $(0, 0, t_l)$, and when it is isotropic, its Gross-Keating epsilon sign is $(-\alpha_l, l)_l$ by definition [GK, Section 3]. Now the formula follows from Lemma 5.2 and the Gross-Keating formula described before the lemma.

Now we assume $l = 2 \neq p$. Since $\tilde{T}(\mu n) \notin \mathrm{Sym}_3(\mathbb{Z}_2)$, $\tilde{T}(\mu n)$ is $\mathrm{GL}_3(\mathbb{Z}_2)$ -equivalent to

$$\mathrm{diag}(\epsilon 2^{t_2}, \begin{pmatrix} A & 1/2 \\ 1/2 & A \end{pmatrix}), \quad A = 0, 1.$$

It is isotropic if and only if $A = 0$ or $A = 1$ and t_2 is even. In each case, the Gross-Keating invariants are $(0, 0, t_2)$ by [Ya2, Proposition B.4]. In the isotropic case, the Gross-Keating epsilon sign is 1 if $A = 0$ and -1 if $A = 1$ by the same proposition. We claim that $A = 0$ if and only if $(-\alpha_2, 2)_2 = 1$, i.e., $\alpha_2 \equiv \pm 1 \pmod{8}$, i.e., the Gross-Keating epsilon sign of

$\tilde{T}(\mu n)$ is again $(-\alpha_2, 2)_2$. Indeed, Lemma 6.1 implies that $a \equiv 3 \pmod{4}$ or $c \equiv 3 \pmod{4}$. Assume without loss of generality $a \equiv 3 \pmod{4}$. In this case $w_0 \equiv 1 \pmod{2}$ and we can take $\alpha_2 = a$. It is easy to see that $\tilde{T}(\mu n)$ is \mathbb{Z}_2 -equivalent to

$$T = \begin{pmatrix} 1 & \frac{1}{2} & \frac{w_1}{2} \\ \frac{1}{2} & \alpha & \frac{1}{4}(b + w_1) \\ \frac{w_1}{2} & \frac{1}{4}(b + w_1) & \frac{1}{4}(c + w_1^2) \end{pmatrix}$$

with $\alpha = \frac{1}{4}(a + 1) \in \mathbb{Z}_2$.

If $(-a, 2)_2 = 1$, i.e., $a \equiv 7 \pmod{8}$, and so $\alpha = \epsilon 2^r$ for some $r \geq 1$ and $\epsilon \in \mathbb{Z}_2^*$. Let β_1 and β_2 are roots of $x^2 + x + \alpha = 0$ with $\beta_1 \in \mathbb{Z}_2^*$ and $\beta_2 \in 2^r \mathbb{Z}_2^*$, and let $L = \oplus \mathbb{Z}_2 e_i$ be the lattice of T . Let

$$f_1 = e_2 + \beta_1 e_1, \quad f_2 = e_2 + \beta_2 e_2.$$

Then it is easy to check that $(f_1, f_2) = -1 + 4\alpha$ and $(f_1, f_1) = (f_2, f_2) = 0$. This implies that $L = (\mathbb{Z}_2 f_1 + \mathbb{Z}_2 f_2) \oplus \mathbb{Z}_2 f_3$ for some $f_3 \in L$. So T and thus $\tilde{T}(\mu n)$ is \mathbb{Z}_2 -equivalent to

$$\text{diag}\left(\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}, \epsilon_1 2^{t_2}\right).$$

If $(-a, 2)_2 = -1$, then $a \equiv 3 \pmod{8}$ and $\alpha \in \mathbb{Z}_2^*$. In this case, it is easy to check by calculation that $L = \mathbb{Z}_2 e_1 \oplus \mathbb{Z}_2 e_2 \oplus \mathbb{Z}_2 f_3$ for some $f_3 \in L$ perpendicular to e_1 and e_2 , and its quadratic form is

$$Q(xe_1 + ye_2 + zf_3) = x^2 + xy + \alpha y^2 + dz^2$$

with $d = Q(f_3)$, and is thus \mathbb{Z}_2 -equivalent to $x^2 + xy + y^2 + d_1 z^2$. So $A = 1$. This proves the claim. The claim implies that the formula is also true for $l = 2$. \square

Proof of Theorem 1.3: Now Theorem 1.3 is clear from Theorem 4.6 and Proposition 5.3

6. COMPUTING $b_1(p)$ AND PROOF OF THEOREM 1.2

The formula for $b_1(p)$ is known to be independent of the choice of the CM type Φ . We choose $\Phi = \{1, \sigma\}$ with $\sigma(\sqrt{\Delta}) = \sqrt{\Delta'}$. Then $\tilde{K} = \tilde{F}(\sqrt{\tilde{\Delta}})$ with

$$(6.1) \quad \tilde{\Delta} = (\sqrt{\Delta} + \sqrt{\Delta'})^2 = \Delta + \Delta' - 2\sqrt{\tilde{D}}.$$

For an integer $0 < n < \sqrt{\tilde{D}}$, let μ and $T(\mu n) = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ be as in Lemma 4.1. Then we have by Lemma 4.1

$$(6.2) \quad \tilde{\Delta} = 2\mu n - Dc - 2\sqrt{\tilde{D}}$$

Lemma 6.1. *Assume the condition (\clubsuit) . For an integer $0 < n < \sqrt{\tilde{D}}$ with $\frac{\tilde{D}-n^2}{4D} \in \mathbb{Z}_{>0}$. let μ and $T(\mu n) = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ be as in Lemma 4.1. Then*

(1) *One has $\frac{\mu n + \sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1} - \mathcal{O}_{\tilde{F}}$ and $\frac{-\mu n + \sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1, '} - \mathcal{O}_{\tilde{F}}$. Here $'$ stands for the Galois conjugation in \tilde{F} .*

- (2) For any prime $p \mid \frac{\tilde{D}-n^2}{D}$, $p \nmid a$ or $p \nmid c$.
 (3) Exactly one of a and c is $0 \pmod{4}$ and the other is $-1 \pmod{4}$.

Proof. (1): When $D \mid n$, one has $D \mid \tilde{D}$, and $d_{\tilde{K}/\tilde{F}} = d'_{\tilde{K}/\tilde{F}}$ and the claim is clear. When $D \nmid n$, one has $\frac{\pm n + \sqrt{\tilde{D}}}{2D} \notin \mathcal{O}_{\tilde{F}}$, and

$$\frac{\tilde{D} - n^2}{4} = \frac{n + \sqrt{\tilde{D}}}{2} \cdot \frac{-n + \sqrt{\tilde{D}}}{2} \in D\mathbb{Z} = d_{\tilde{K}/\tilde{F}} d'_{\tilde{K}/\tilde{F}}.$$

So there is a unique $\nu = \pm 1$ such that

$$\frac{\nu n + \sqrt{\tilde{D}}}{2} \in d'_{\tilde{K}/\tilde{F}}, \quad \frac{-\nu n + \sqrt{\tilde{D}}}{2} \in d_{\tilde{K}/\tilde{F}}.$$

On the other hand, $\tilde{\Delta} \in d_{\tilde{K}/\tilde{F}}$ implies $\mu n - \sqrt{\tilde{D}} \in d_{\tilde{K}/\tilde{F}}$. So $(\mu - \nu)n \in d_{\tilde{K}/\tilde{F}}$ and thus $(\mu - \nu)n \equiv 0 \pmod{D}$. So $\mu = \nu$. Now it is easy to see

$$\frac{\mu n + \sqrt{\tilde{D}}}{2D} \in d_{\tilde{K}/\tilde{F}}^{-1} - \mathcal{O}_{\tilde{F}}, \quad \frac{-\mu n + \sqrt{\tilde{D}}}{2D} \notin d_{\tilde{K}/\tilde{F}}^{-1, \prime} - \mathcal{O}_{\tilde{F}}.$$

(2): If $p \mid a, c$, then $p \mid ac - b^2 = \frac{\tilde{D}-n^2}{D}$ implies $p \mid b$, and thus

$$p \mid n = -\nu(a + Db + \frac{D^2 - D}{4}c).$$

This implies $p \mid \tilde{D}$. But this causes a contradiction: $p^2 \mid ac - b^2 = \frac{\tilde{D}-n^2}{D}$.

(3): Since K/F is unramified at primes of F over 2 under the condition (\clubsuit), there are integers x and y , not both even, such that

$$\Delta \equiv (x + y \frac{1 + \sqrt{D}}{2})^2 \pmod{4}.$$

By Lemma 4.1, this implies

$$-a = (D+1)b - \frac{D^2 - D}{4}c - Dc \frac{1 + \sqrt{D}}{2} \equiv x^2 + y^2 \frac{D-1}{4} + (y^2 + 2xy) \frac{1 + \sqrt{D}}{2} \pmod{4}.$$

So (since $D \equiv 1 \pmod{4}$)

$$(6.3) \quad a + x^2 + 2b + \frac{D-1}{4}(c + y^2) \equiv 0 \pmod{4},$$

$$(6.4) \quad 2xy + y^2 + c \equiv 0 \pmod{4}.$$

When x is even, y has to be odd. So $c \equiv -1 \pmod{4}$ and a is even. Since

$$(6.5) \quad ac - b^2 = \det T(\mu n) = \frac{\tilde{D} - n^2}{D} \equiv 0 \pmod{4},$$

one has $a \equiv 0 \pmod{4}$ and $b \equiv 0 \pmod{2}$.

When x is odd and y is even, (6.3), (6.4), and (6.5) imply $a + 1 \equiv c \equiv 0 \pmod{4}$.

When both x and y are odd, (6.4) implies $c \equiv 1 \pmod{4}$. So (6.3) implies that a is odd and thus b is odd. Now (6.5) implies $a \equiv 1 \pmod{4}$ and that b is odd. So (6.3) implies

$D \equiv 1 \pmod{8}$. But this implies that $-\mu n = a + Db + \frac{D^2-D}{4}c$ is even, which is impossible since \tilde{D} is odd. So this case is impossible. \square

It is easy to see from the definition that $b_1(p) = 0$ unless there is $n > 0$ with $\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$. This implies in particular p is split in \tilde{F} or $p|\tilde{D}$ is ramified in \tilde{F} . For a fixed $n > 0$ with $\frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}$, fix a sign $\mu = \pm 1$ such that $T(\mu n)$ exists as in Lemma 4.1. In the split case, we choose the splitting $p\mathcal{O}_{\tilde{F}} = \mathfrak{p}\mathfrak{p}'$ such that

$$(6.6) \quad t_{\mu n} = \frac{\mu n + \sqrt{\tilde{D}}}{2D} \in \mathfrak{p}d_{\tilde{K}/\tilde{F}}^{-1}.$$

So

$$(6.7) \quad \text{ord}_{\mathfrak{p}} t_{\mu n} = \text{ord}_p \frac{\tilde{D} - n^2}{4D}, \quad \text{ord}_{\mathfrak{p}'}(t_{\mu n}) = 0 \text{ or } -1.$$

In the ramified case $p\mathcal{O}_{\tilde{F}} = \mathfrak{p}^2$, the above two equations also hold (forgetting the one with \mathfrak{p}'). With this notation, we have by (1.4)

$$(6.8) \quad b_1(p) = \sum_{0 < n < \sqrt{\tilde{D}}, \frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D} - n^2}{4D} + 1) \sum_{\mu} b(p, \mu n)$$

where

$$(6.9) \quad b(p, \mu n) = \begin{cases} 0 & \text{if } \mathfrak{p} \text{ is split in } \tilde{K}, \\ \rho(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) & \text{if } \mathfrak{p} \text{ is not split in } \tilde{K}. \end{cases}$$

Assume now that \mathfrak{p} is not split in \tilde{K} . Notice that

$$\rho(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = \prod_{\mathfrak{l}} \rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1})$$

where the product runs over all prime ideals \mathfrak{l} of \tilde{F} , and

$$(6.10) \quad \rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = \begin{cases} 1 & \text{if } \mathfrak{l} \text{ is ramified in } \tilde{K}, \\ \frac{1 + (-1)^{\text{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1})}}{2} & \text{if } \mathfrak{l} \text{ is inert in } \tilde{K}, \\ 1 + \text{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) & \text{if } \mathfrak{l} \text{ is split in } \tilde{K}. \end{cases}$$

Notice first that $\rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = 1$ unless $\text{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) \geq 1$. In particular it is 1 unless $l|\frac{\tilde{D}-n^2}{4Dp}$ where l is the prime under \mathfrak{l} . So we assume that $l|\frac{\tilde{D}-n^2}{4Dp}$. This implies that either $l|\tilde{D}$ is ramified in \tilde{F} or $l = \mathfrak{l}'$ is split in \tilde{F} . In the split case, we again choose the splitting $l\mathcal{O}_{\tilde{F}} = \mathfrak{l}'$ so that

$$(6.11) \quad \text{ord}_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = \text{ord}_l \frac{\tilde{D} - n^2}{4Dp} = \text{ord}_l \frac{\det T(\mu n)}{4p}, \quad \text{ord}_{\mathfrak{l}'}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = 0.$$

Lemma 6.2. *Let the notation be as above. Assume $\mathfrak{l} \neq d_{\tilde{K}/\tilde{F}}$ and that $T(\mu n)$ is $\mathrm{GL}_2(\mathbb{Z}_l)$ -equivalent to $\mathrm{diag}(\alpha_l, \alpha_l^{-1} \det T(\mu n))$ with $\alpha_l \in \mathbb{Z}_l^*$. Then \tilde{K}/\tilde{F} is split (resp. inert) at \mathfrak{l} if and only if $(-\alpha_l, l)_l = 1$ (resp. -1).*

Proof. Since $\mathfrak{l} \neq d_{\tilde{K}/\tilde{F}}$, \mathfrak{l} is either split or inert in \tilde{K} . We first take care of a very special case $\mathfrak{l} = d'_{\tilde{K}/\tilde{F}} \neq d_{\tilde{K}/\tilde{F}}$. In this case, $l = D \nmid n$. So

$$\tilde{\Delta} = 2\mu n - Dc - 2\sqrt{\tilde{D}} \equiv 2\mu n - 2\sqrt{\tilde{D}} \equiv 4\mu n \equiv -4a \pmod{\mathfrak{l}}$$

So $l \nmid a$, and $\tilde{K} = \tilde{F}(\sqrt{\tilde{\Delta}})$ is split at \mathfrak{l} if and only if $(-a, l)_l = 1$. In this case $\alpha_l = a$.

Now we can assume $l \neq D$. We divide the proof into three cases and more subcases.

Case 1: First we assume that $l|\tilde{D}$ is ramified in \tilde{F} . In this case, $l\mathcal{O}_{\tilde{F}} = \mathfrak{l}^2$, $l|n$, and

$$\tilde{\Delta} = 2\mu n - Dc - 2\sqrt{\tilde{D}} \equiv -Dc \pmod{\mathfrak{l}}.$$

Since $\mathrm{ord}_l \frac{\tilde{D}-n^2}{4D} = 1$, it is easy to check $l \nmid c$ and thus $\tilde{\Delta} \not\equiv 0 \pmod{\mathfrak{l}}$. Since $\tilde{\Delta}\tilde{\Delta}' = Dv^2$, one has

$$\tilde{\Delta}^2 \equiv Dv^2 \pmod{\mathfrak{l}}$$

and

$$1 \equiv -\tilde{\Delta}cv^2 \pmod{\mathfrak{l}}.$$

So $\tilde{K} = \tilde{F}(\sqrt{\tilde{\Delta}})$ is split at \mathfrak{l} if and only if $(-c, l)_l = 1$. Notice that $\alpha_l = c$ in the case.

Case 2: Next we assume that $l \nmid 2\tilde{D}$. So l is split as discussed above. In this case, either $\mathfrak{l} \nmid \tilde{\Delta}$ or $\mathfrak{l} \nmid (\tilde{\Delta})'$.

Subcase 1: We first assume $\mathfrak{l} \nmid \tilde{\Delta}$. Since $t_{\mu n} \in \mathfrak{l}$, one has

$$\tilde{\Delta} = 2\mu n - Dc - 2\sqrt{\tilde{D}} \equiv 4\mu n - Dc \pmod{4\mathfrak{l}} \equiv -\alpha \pmod{4\mathfrak{l}}$$

with $\alpha = 4a + 4Db + D^2c$. So over $\tilde{F}_l = \mathbb{Q}_l$, one has

$$(\tilde{\Delta}, l)_l = (-\alpha, l)_l.$$

So $(-\alpha, l)_l = 1$ (resp. -1) if and only if \tilde{K}/\tilde{F} is split (resp. inert) at \mathfrak{l} . On the other hand,

$$\begin{pmatrix} 2 & D \\ 1 & \frac{D+1}{2} \end{pmatrix} T(\mu n) \begin{pmatrix} 2 & 1 \\ D & \frac{D+1}{2} \end{pmatrix} = \begin{pmatrix} \alpha & * \\ * & * \end{pmatrix},$$

$T(\mu n)$ is $\mathrm{GL}_2(\mathbb{Z}_l)$ -equivalent to $\mathrm{diag}(\alpha, \alpha^{-1} \det T(\mu n))$.

Subcase 2: We now assume $\mathfrak{l} \nmid \tilde{\Delta}'$. Since $\tilde{\Delta}\tilde{\Delta}' = Dv^2$ for some integer v , we see that

$$(\tilde{\Delta}, l)_l = (\tilde{\Delta}', l)_l (D, l)_l.$$

On the other hand,

$$\tilde{\Delta}' = 2\mu n - Dc + 2\sqrt{\tilde{D}} \equiv -Dc \pmod{4\mathfrak{l}},$$

one sees that $(\tilde{\Delta}, l)_l = (-c, l)_l$ and $l \nmid c$. Since $T(\mu n)$ is $\mathrm{GL}_2(\mathbb{Z}_l)$ -equivalent to $\mathrm{diag}(c, c^{-1} \det T(\mu n))$ in this case, the lemma is true too.

Case 3: Finally, we deal with the case $l = 2$. When $2 \nmid c$, the same argument as in Subcase 2 above gives the lemma. When $2|c$, the situation is more complicated and

technical. First, $ac - b^2 = \frac{\tilde{D} - n^2}{D} \equiv 0 \pmod{8}$ implies that $4|c$ and $2|b$. We choose the splitting $2 = \mathfrak{l}'$ as in (6.11).

Subcase 1: If $c = 8c_1 \equiv 0 \pmod{8}$, then $b = 4b_1 \equiv 4$ and

$$\begin{aligned} -\frac{\tilde{\Delta}}{4} &= -\mu n + 2Dc_1 + \frac{\mu n + \sqrt{\tilde{D}}}{2} \\ &= a + 4Db_1 + 2D^2c_1 + \frac{\mu n + \sqrt{\tilde{D}}}{2} \\ &\not\equiv 0 \pmod{\mathfrak{l}}. \end{aligned}$$

Notice that

$$(6.12) \quad \left(\frac{x + y\sqrt{\tilde{D}}}{2}\right)^2 = \left(\frac{x - \mu ny}{2}\right)^2 + xy \frac{\mu n + \sqrt{\tilde{D}}}{2} + y^2 \frac{\tilde{D} - n^2}{4}.$$

So $\tilde{K} = \tilde{F}(\sqrt{\tilde{\Delta}})$ is split at \mathfrak{l} if and only if there is $\frac{x+y\sqrt{\tilde{D}}}{2} \in \mathcal{O}_{\tilde{F}}$ with x and y odd such that

$$\frac{\tilde{\Delta}}{4} \equiv \left(\frac{x + y\sqrt{\tilde{D}}}{2}\right)^2 \pmod{4\mathfrak{l}},$$

i.e.,

$$a + 4Db_1 + 2D^2c_1 + y^2 \frac{\tilde{D} - n^2}{4} + \left(\frac{x - \mu ny}{2}\right)^2 + (xy + 1) \frac{\mu n + \sqrt{\tilde{D}}}{2} \equiv 0 \pmod{4\mathfrak{l}}.$$

Notice that $\frac{\tilde{D} - n^2}{4} = D(2ac_1 - 4b_1^2)$. So $\tilde{K} = \tilde{F}(\sqrt{\tilde{\Delta}})$ is split at \mathfrak{l} if and only if there are odd integers x and y such that

$$a + 4D(b_1 - b_1^2) + 2Dc_1(D + a) + \left(\frac{x - \mu ny}{2}\right)^2 + (xy + 1) \frac{\mu n + \sqrt{\tilde{D}}}{2} \equiv 0 \pmod{4\mathfrak{l}}.$$

That is

$$a + \left(\frac{x + ay}{2}\right)^2 + (xy + 1) \frac{\mu n + \sqrt{\tilde{D}}}{2} \equiv 0 \pmod{4\mathfrak{l}},$$

since $D + a \equiv 0 \pmod{4}$ and $-\mu n \equiv a \pmod{4}$. In particular, one has to have $x + ay \equiv 2 \pmod{4}$, and thus $xy \equiv -1 \pmod{4}$ (recall that $a \equiv -1 \pmod{4}$). So the above congruence is equivalent to

$$a + \left(\frac{x + ay}{2}\right)^2 \equiv 0 \pmod{4\mathfrak{l}},$$

i.e., $(-a, 2)_2 = 1$. So \tilde{K}/\tilde{F} is split if and only if $(-a, 2)_2 = 1$.

Subcase 2: Now we assume that $c = 4c_1$ with c_1 odd. In this case, $b = 2b_1$ with b_1 odd, and $\frac{\tilde{\Delta}}{4} \equiv 0 \pmod{\mathfrak{l}}$, not easy to deal with. We switch to $\tilde{\Delta}'$. We have

$$(6.13) \quad \frac{\tilde{\Delta}'}{4} = \frac{\mu n + \sqrt{\tilde{D}}}{2} - Dc_1 \not\equiv 0 \pmod{\mathfrak{l}}.$$

Since $\tilde{\Delta}\tilde{\Delta}' = Dv^2$ if $\Delta = \frac{u+v\sqrt{D}}{2}$, $\tilde{K} = \tilde{F}(\sqrt{\tilde{\Delta}}) = \tilde{F}(\sqrt{D\tilde{\Delta}'})$ is split at \mathfrak{l} if and only if there is odd integers x and y such that

$$\frac{D\tilde{\Delta}'}{4} \equiv \left(\frac{x+y\sqrt{\tilde{D}}}{2}\right)^2 \equiv \pmod{4\mathfrak{l}}.$$

By (6.12) and (6.13), this is equivalent to

$$-c_1 \equiv \left(\frac{x-\mu ny}{2}\right)^2 + D(ac_1 - b_1^2) + (xy - D)\frac{\mu n + \sqrt{\tilde{D}}}{2} \pmod{4\mathfrak{l}}.$$

Since

$$-a + c_1 + D(ac_1 - b_1^2) = D(a+1)(c_1 - 1) + (D-1)(a - c_1) + D(1 - b_1^2) \equiv 0 \pmod{4\mathfrak{l}},$$

the above congruence is equivalent to

$$(6.14) \quad -a \equiv \left(\frac{x-\mu ny}{2}\right)^2 + (xy - D)\frac{\mu + \sqrt{\tilde{D}}}{2} \pmod{4\mathfrak{l}}.$$

In particular, $\frac{x-\mu ny}{2}$ has to be odd. Since

$$-\mu n = a + 2Db_1 + (D^2 - D)c_1 \equiv a + 2 \pmod{4},$$

this means $\frac{x+ay}{2} \equiv 0 \pmod{2}$, and thus $xy \equiv 1 \pmod{4}$. So (6.14) is equivalent to

$$-a \equiv \left(\frac{x-\mu ny}{2}\right)^2 \pmod{4\mathfrak{l}}.$$

Therefore, \tilde{K}/\tilde{F} is split at \mathfrak{l} if and only if $(-a, 2)_2 = 1$. This finally finishes the proof of the lemma. \square

Theorem 6.3. *One has*

$$(6.15) \quad b_1(p) = \sum_{0 < n < \sqrt{\tilde{D}}, \frac{\tilde{D}-n^2}{4D} \in p\mathbb{Z}_{>0}} (\text{ord}_p \frac{\tilde{D}-n^2}{4D} + 1) \sum_{\mu} \beta(p, \mu n),$$

where $\beta(p, \mu n)$ is given as in Theorem 1.3.

Proof. The discussion between Lemma 6.1 and Lemma 6.2 gives (6.15) with

$$b(p, \mu n) = \prod_l b_l(p, \mu n).$$

Here for $l \neq p$

$$b_l(p, n) = \prod_{\mathfrak{l}|\mathfrak{l}} \rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}).$$

For $l = p$, $p\mathcal{O}_{\tilde{F}} = d_{\tilde{K}/\tilde{F}} d'_{\tilde{K}/\tilde{F}}$. Write $\mathfrak{p} = d'_{\tilde{K}/\tilde{F}}$, then

$$b_p(p, \mu n) = \begin{cases} 0 & \text{if } \mathfrak{p} \text{ split in } \tilde{K}, \\ \rho_{\mathfrak{p}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) & \text{if } \mathfrak{p} \text{ not split in } \tilde{K}. \end{cases}$$

When $l \nmid \frac{\tilde{D}-n^2}{4D}$, one has clearly $b_l(p, \mu n) = 1$.

When $l = p$,

$$\begin{aligned} b_p(p, \mu n) &= \begin{cases} 0 & \text{if } \mathfrak{p} \text{ is split in } \tilde{K}, \\ \frac{1+(-1)^{t_p-1}}{2} & \text{if } \mathfrak{p} \text{ is not split in } \tilde{K}, \end{cases} \\ &= \frac{1 - (-\alpha_p, p)_p^{t_p}}{2} \\ &= \beta_p(p, \mu n) \end{aligned}$$

as claimed.

When $l \mid \frac{\tilde{D}-n^2}{4D}$, but $l \neq p$, l is split in \tilde{F} or $l \mid \tilde{D}$ is ramified in \tilde{K} . In the split case, we choose the splitting $l\mathcal{O}_{\tilde{F}} = \mathfrak{l}'$ so that (6.11) holds, and $\rho_{\nu}(t_n d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1}) = 1$. In either case, $b_l(p, \mu n) = \rho_{\mathfrak{l}}(t_{\mu n} d_{\tilde{K}/\tilde{F}} \mathfrak{p}^{-1})$. Now Lemma 6.2 and (6.10) give the desired formula for $b_l(p, \mu n)$. \square

Proof of Theorem 1.2: Now Theorem 1.2 follows from Theorems 1.3 and 6.3.

7. PROOF OF THEOREM 1.5

A holomorphic Hilbert modular form for $\mathrm{SL}_2(\mathcal{O}_F)$ is called *normalized integral*, if all its Fourier coefficients at the cusp ∞ are rational integers with greatest common divisor 1.

Lemma 7.1. *Assume $D = 5, 13$ or 17 . Then for every integer $m > 0$, there is a positive integer $a(m) > 0$ and a normalized integral holomorphic Hilbert modular form Ψ_m such that*

$$\mathrm{div} \Psi_m = a(m) \mathcal{T}_m.$$

Proof. Let $S_2^+(D, (\frac{D}{n}))$ be the space of elliptic modular forms of weight 2, level D , and Nebentypus character $(\frac{D}{n})$ such that its Fourier coefficients satisfy $a(n) = 0$ if $(\frac{D}{n}) = -1$. Then a well-known theorem of Hecke asserts $\dim S_2^+(D, (\frac{D}{n})) = 0$ for primes $D = 5, 13, 17$. By a Serre duality theorem of Borchers [Bo2] and Borchers's lifting theorem [Bo1] (see [BB] in our special setting), there is Hilbert modular form Ψ_m such that $\mathrm{div} \Psi_m(\mathbb{C}) = T_m$ and sufficient large power of Ψ_m is a normalized integral Hilbert modular form. Replacing Ψ_m by a sufficient large power if necessary we may assume that Ψ_m is a normalized integral holomorphic Hilbert modular form. So $\mathrm{div} \Psi_m$ is flat over \mathbb{Z} and thus $\mathrm{div} \Psi_m = a(m) \mathcal{T}_m$. \square

Proof of Theorem 1.5: Let $\hat{\omega} = (\omega, \|\cdot\|_{\mathrm{Pet}})$ be the metrized Hodge bundle on $\tilde{\mathcal{M}}$ with the Petersson metric defined in Section 2. Let $\tilde{\mathcal{T}}_1$ be the closure of \mathcal{T}_1 in $\tilde{\mathcal{M}}$. Let Ψ_1 be a normalized integral Hilbert modular form of weight $c(1)$ given in Lemma 7.1. Then Ψ_1 can be extended to a section of $\omega^{c(1)}$, still denoted by Ψ_1 such that

$$\mathrm{div} \Psi = a(1) \tilde{\mathcal{T}}_1.$$

Since $\mathcal{CM}(K)$ never intersects with the boundary $\tilde{\mathcal{M}} - \mathcal{M}$, $\tilde{\mathcal{T}}_1.\mathcal{CM}(K) = \mathcal{T}_1.\mathcal{CM}(K)$. So

$$\begin{aligned} c(1)\mathrm{ht}_{\hat{\omega}}(\mathcal{CM}(K)) &= \mathrm{ht}_{\widehat{\mathrm{div}}(\Psi_1)}(\mathcal{CM}(K)) \\ &= a(1)\mathcal{CM}(K).\mathcal{T}_1 - \frac{2}{W_K} \sum_{z \in \mathrm{CM}(K)} \log \|\Psi_1(z)\|_{\mathrm{Pet}} \\ &= \frac{a(1)}{2}b_1 - \frac{a(1)}{2} \frac{W_{\tilde{K}}}{W_K} b_1 + \frac{c(1)}{2} \frac{W_{\tilde{K}}}{W_K} \Lambda(0, \chi_{\tilde{K}/\tilde{F}}) \beta(\tilde{K}/\tilde{F}) \end{aligned}$$

by Theorem 1.2 and [BY, Theorem 1.4]. It is not hard to check that

$$W_K = W_{\tilde{K}} = \begin{cases} 10 & \text{if } K = \tilde{K} = \mathbb{Q}(\zeta_5), \\ 2 & \text{otherwise.} \end{cases}$$

Let $M = K\tilde{K}$ be the Galois closure of K (and \tilde{K}) over \mathbb{Q} , view both $\chi_{\tilde{K}/\tilde{F}}$ and $\chi_{K/F}$ as characters of $\mathrm{Gal}(M/\tilde{F})$ and $\mathrm{Gal}(M/F)$ respectively by class field theory. Then

$$\pi = \mathrm{Ind}_{\mathrm{Gal}(M/\tilde{F})}^{\mathrm{Gal}(M/\mathbb{Q})} \chi_{\tilde{K}/\tilde{F}} = \mathrm{Ind}_{\mathrm{Gal}(M/F)}^{\mathrm{Gal}(M/\mathbb{Q})} \chi_{K/F}$$

is the unique two dimensional irreducible representation of $\mathrm{Gal}(M/\mathbb{Q})$ when K is not cyclic (when K is cyclic, the identity is trivial). So

$$L(s, \chi_{\tilde{K}/\tilde{F}}) = L(s, \chi_{K/F}) = L(s, \pi),$$

and thus $\beta(\tilde{K}/\tilde{F}) = \beta(K/F)$. Finally, [BY, (9.2)] asserts

$$\Lambda(0, \chi_{\tilde{K}/\tilde{F}}) = \frac{2\#\mathrm{CM}(K)}{W_K}.$$

So

$$h_{\hat{\omega}}(\mathcal{CM}(K)) = \frac{\#\mathrm{CM}(K)}{W_K} \beta(K/F).$$

Combining this with (2.7), one obtains

$$(7.1) \quad h_{\mathrm{Fal}}(A) = \frac{1}{2} \beta(K/F).$$

This proves Theorem 1.5.

REFERENCES

- [Ad] *G. Anderson*, Logarithmic derivatives of Dirichlet L -functions and the periods of abelian varieties. *Compositio Math.* **45**(1982), 315–332.
- [Bo1] *R. E. Borcherds*, Automorphic forms with singularities on Grassmannians, *Invent. Math.* **132** (1998), 491–562.
- [Bo2] *R. E. Borcherds*, The Gross-Kohnen-Zagier theorem in higher dimensions, *Duke Math. J.* **97** (1999), 219–233.
- [BB] *J. H. Bruinier and M. Bundschuh*, On Borcherds products associated with lattices of prime discriminant, *Ramanujan J.* **7** (2003), 49–61.
- [BBK] *J. Bruinier, J. Burgos Gill, and U. Kühn*, Borcherds products and arithmetic intersection theory on Hilbert modular surfaces, *Duke Math. J.* **139** (2007), 1–88.

- [BY] *J. H. Bruinier and T. Yang*, CM values of Hilbert modular functions, *Invent. Math.* **163** (2006), 229–288.
- [Co] *P. Colmez*, Périodes des variétés abéliennes à multiplication complexe, *Ann. Math.*, 138(1993), 625–683.
- [DP] *P. Deligne and G. Pappas*, Singularities des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant, *Compos. Math.* 90 (1994), 5979.
- [Fa] *G. Faltings*, Finiteness theorems for abelian varieties over number fields. Translated from the German original [*Invent. Math.* 73 (1983), 349–366; *ibid.* 75 (1984), 381;] by Edward Shipz. *Arithmetic geometry* (Storrs, Conn., 1984), 9–27, Springer, New York, 1986.
- [Go] *E. Goren*, Lectures on Hilbert modular varieties and modular forms, CRM monograph series 14, 2001.
- [Gr] *B. Gross*, On the periods of abelian integrals and a formula of Chowla and Selberg. With an appendix by David E. Rohrlich. *Invent. Math.* **45** (1978), 193–211.
- [GK] *B. Gross and K. Keating*, On the intersection of modular correspondences, *Invent. Math.* **112**(1993), 225–245.
- [GZ1] *B. Gross and D. Zagier*, On singular moduli. *J. Reine Angew. Math.* **355** (1985), 191–220.
- [GZ2] *B. Gross and D. Zagier*, Heegner points and derivatives of L -series. *Invent. Math.* **84** (1986), 225–320.
- [HZ] *F. Hirzebruch and D. Zagier*, Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus, *Invent. Math.* **36** (1976), 57–113.
- [Ig] *J.-I. Igusa*, Arithmetic Variety of Moduli for Genus Two. *Ann. Math.* 72, (1960), 612–649
- [La] *K. Lauter*, Primes in the denominators of Igusa Class Polynomials, preprint, pp3, <http://www.arxiv.org/math.NT/0301240/>.
- [Ku1] *S. Kudla*, Central derivatives of Eisenstein series and height pairings. *Ann. of Math.* (2) **146** (1997), 545–646.
- [Ku2] *S. Kudla*, Special cycles and derivatives of Eisenstein series, in Heegner points and Rankin L -series, 243–270, *Math. Sci. Res. Inst. Publ.*, 49, Cambridge Univ. Press, Cambridge, 2004.
- [KR1] *S. Kudla and M. Rapoport*, Arithmetic Hirzebruch Zagier cycles, *J. reine angew. Math.*, **515** (1999), 155–244.
- [KR2] *S. Kudla and M. Rapoport*, Cycles on Siegel 3-folds and derivatives of Eisenstein series, *Annales Ecole. Norm. Sup.* **33** (2000), 695–756.
- [KRY1] *S. Kudla, M. Rapoport, and T.H. Yang*, Derivatives of Eisenstein Series and Faltings heights, *Comp. Math.*, **140** (2004), 887–951.
- [KRY2] *S. Kudla, M. Rapoport, and T.H. Yang*, Modular forms and special cycles on Shimura curves, *Annals of Math. Studies series*, vol 161, 2006, Princeton Univ. Publ.
- [Se] *J.-P. Serre*, A course in Arithmetic, GTM **7**, Springer-Verlag, New York, 1973.
- [Vo] *I. Vollaard*, On the Hilbert-Blumenthal moduli problem, *J. Inst. Math. Jussieu* 4 (2005), 653–683.
- [We1] *T. Wedhorn*, Calculation of representation densities, Chapter 15 in ARGOS seminar on Intersections of Modular Correspondences, p. 185–196, to appear in *Asterisque*.
- [We2] *T. Wedhorn*, The genus of the endomorphisms of a supersingular elliptic curve, Chapter 5 in ARGOS seminar on Intersections of Modular Correspondences, p. 37–58, to appear in *Asterisque*.
- [Ya1] *T.H. Yang*, An explicit formula for local densities of quadratic forms, *J. Number Theory* **72**(1998), 309–356.
- [Ya2] *T.H. Yang*, Local densities of 2-adic quadratic forms, *J. Number Theory* **108**(2004), 287–345.
- [Ya3] *T. H. Yang*, Chowla-Selberg Formula and Colmez’s Conjecture, preprint, 2007, pp17.
- [Ya4] *T. H. Yang*, Arithmetic Intersection on a Hilbert Modular Surface and Faltings’ Height, preprint, 2008, pp45.
- [Yu] *C.F. Yu*, The isomorphism classes of abelian varieties of CM types, *Jour. pure and Appl. Algebra*, **187**(2004), 305–319.

- [Zh1] *S. W. Zhang*, Heights of Heegner cycles and derivatives of L-series, *Invent. Math.* **130** (1997), 99–152.
- [Zh2] *S. W. Zhang*, Heights of Heegner points on Shimura curves, *Ann. of Math. (2)* **153** (2001), 27–147.
- [Zh3] *S. W. Zhang*, Gross-Zagier formula for $GL(2)$, *Asian. J. Math.* 5 (2001), 183–290; II, Heegner points and Rankin L-series, 191–214, *Math. Sci. Res. Inst. Publ.*, 49, Cambridge Univ. Press, Cambridge, 2004.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN MADISON, VAN VLECK HALL, MADISON, WI 53706, USA

E-mail address: `thyang@math.wisc.edu`